*********CCNA Notes**********

Introduction of CCNA

CCNA (Cisco Certified Network Associate) is a certification name for computer network engineers. It is provided by the company named Cisco Systems. It is valid for students related to BCA, BScIT, B.Tech, etc. It helps to become familiar with broad range of networking concepts like OSI models, IP addressing, Router and Switch handling, Network security, etc.

Exam Process :-

What a student who would like to get global certification should do?

1. Get Training
2. Register for exam through any authorized testing center
3. Exam code : 200-301
4. Exam duration – 120 minutes
5. Exam Questions – 40-50
6. Exam Fee - $300
7. Exam Mode – Online at center
8. Certificate validity – 3 years

Job Opportunity:

Cisco certified candidates can get a job at different companies as Network Engineer, Network Administrator, etc.

Switch:

The device supports simultaneous, parallel connections between Ethernet segments. Switched connections between Ethernet segments last only for the duration of the packet. New connections can be made between different segments for the next packet.

The device solves congestion problems caused by high-bandwidth devices and a large number of users by assigning each device to its own 10-, 100-, 1000-Mbps, or 10-Gigabit collision domain. Because each LAN port connects to a separate Ethernet collision domain to achieve full access to the bandwidth.

Because collisions cause significant congestion in Ethernet networks, an effective solution is full-duplex communication. Typically, 10/100-Mbps Ethernet operates in half-duplex mode, which means that stations can either receive or transmit. In full-duplex mode, which is configurable on these interfaces, two stations can transmit and receive at the same time. When packets can flow in both directions simultaneously, the effective Ethernet bandwidth doubles. 1/10-Gigabit Ethernet operates in full duplex only.

Types:

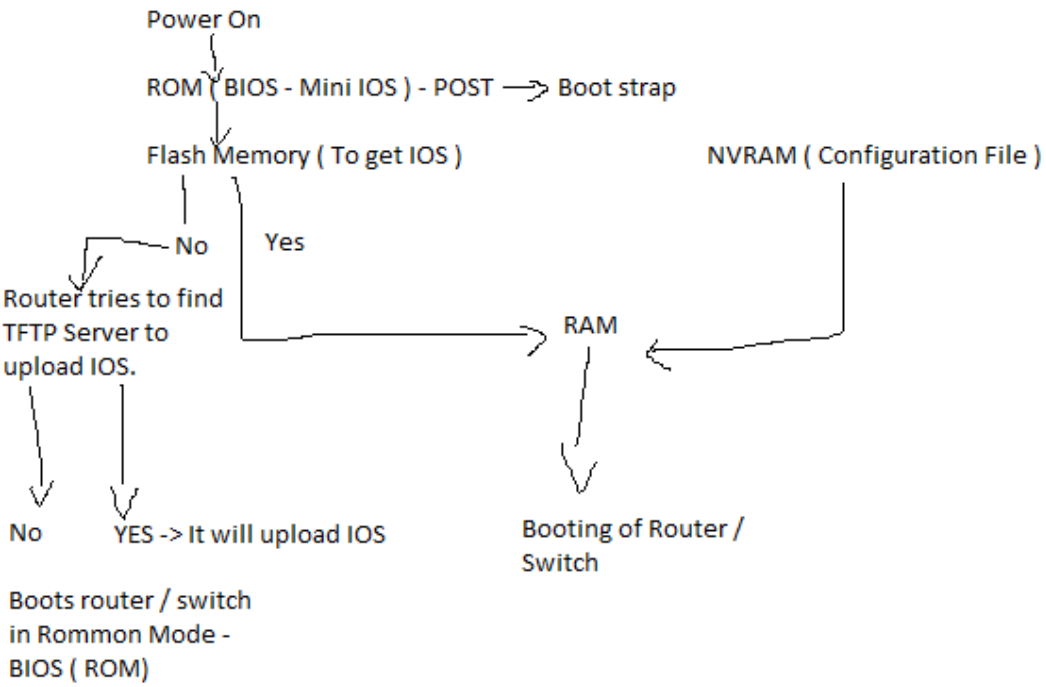
1. L2 Switch
    a. Multiple Ethernet, Fast Ethernet, Gigabit Ethernet, 10G Ethernet ports
    b. It creates MAC Table.
    c. L2 Switch can be Manageable or Un-manageable.
    d. Speed – 10 Mbps, 100 Mbps, 1000 Mbps, 10 Gbps
    e. Transmission Mode – Full Duplex
    f. It has different Features : VLAN, Trunking, Loop free, Port Security
    g. L2 Switch can be with PoE Ports.
2. L3 Switch
    a. Multiple Ethernet, Fast Ethernet, Gigabit Ethernet, 10G Ethernet ports
    b. It creates Routing Table.
    c. Speed – 10 Mbps, 100 Mbps, 1000 Mbps, 10 Gbps
    d. Transmission Mode – Full Duplex
    e. It can connect two or more different networks.
    f. Features : IP Routing, IP Packet Filteration
3. Fiber Switch
    a. It has multiple fiber port – SC, ST, SMA
    b. It works on light signal
    c. Ethernet Switch are also available with few fiber ports.
    d. It is mostly used in telecom network & cloud infracture
    e. Speed – 100 Gbps (Upcoming 400 Gbps)

Internal Components of Router / L2 Switch

1. SMPS – AC to DC power supply
2. Mother Board –Circuit Board
3. Processor –

4. ROM – BIOS (Mini IOS)
5. RAM –
6. NVRAM – (It keeps configuration file)
7. Flash Memory (HDD)- IOS (Internetwork Operating System)

Booting Process of router / Switch :



Different Mode of router / Switch :

Router> -> User Execute Mode

Router# ->Previlleged Mode (Mostly configuration is checked)

Router(confg)# ->Global Configuration Mode (Different Configuration can be done)

Basic Configuration of Router/Switch:

Few Concepts to run commands –

1. Only few characters can be typed
   Enter
   Enable
   Exit
   To execute enable -> Ena
   To complete word press Tab
2. We use ? to know about the next word of command
   What ?
   Is
   Are
   Had
   Has
3. History
4. Commands are not case sensitive

Basic Commands :-

1. Router>enable (To go into previllaged mode)
   Router#
2. Router#Show version
3. Router#Show flash
4. Router#Show running-configuration
5. Router#Show startup-configuration
6. Router#Show clock
7. Router#Show ip route
8. Router#conf t
9. Router(config)#

Router –

Establish connection between diff networks.

Works at L3

Works on IP packets

Provides IP routing. - It is a process by which a routing table is created. This routing table helps to provide the best path to different destination networks.

Creates IP routing table and keeps the best path for different destination networks.

It also provides security for IP packet filtration with ACL.

Interfaces / Ports:-

1. Ethernet, Fast Ethernet, Gigabit Ethernet – Used to connect with LAN, WAN or router
2. Serial Interface – Used to connect with router or WAN
3. ISDN Interface(BRI/PRI) – Used to connect with ISDN line.
4. Console Port - Used for configuration.

Types of router:-

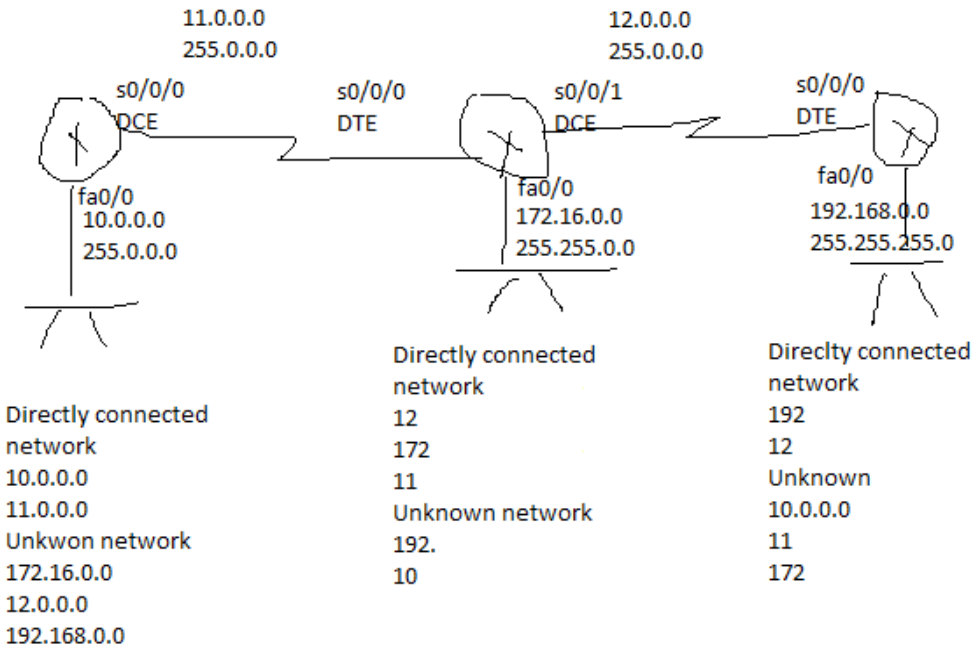
1. De-modular Router – All ports are fixed. Ex. 2600
2. Modular Router – Free slots are available to connect different cards. Ex- 1800, 1900,900,7200, etc.

Types of routing:

1. **Static Routing**
2. **Static Default**
3. **Dynamic routing**

Static Routing :

It is a process by which routes are defined at routers manually. It can be useful for a small network. It increases the administrative task.



Router 1

Router>enable

Router#conf t

Router(config)#

Router(config)#hostname r1
Router(config)#int fa0/0
Router(config)#ip add 10.0.0.1 255.0.0.0
Router(config)#no shut
Router(config)#int s0/0/0
Router(config)#ip add 11.0.0.1 255.0.0.0
Router(config)#clock rate 64000
Router(config)#no shut
Router(config)#ip route 12.0.0.0 255.0.0.0 11.0.0.2

Router(config)#ip route 172.16.0.0 255.255.0.0 11.0.0.2
Router(config)#ip route 192.168.0.0 255.255.255.0 11.0.0.2

Router 2

Router(config)#hostname r2

Router(config)#int fa0/0

Router(config)#ip add 172.16.0.1 255.255.0.0

Router(config)#no shut

Router(config)#int s0/0/0

Router(config)#ip add 11.0.0.2 255.0.0.0

Router(config)#no shut

Router(config)#int s0/0/1

Router(config)#ip add 12.0.0.1 255.0.0.0

Router(config)#clock rate 64000

Router(config)#no shut

Router(config)#ip route 10.0.0.0 255.0.0.0 11.0.0.1

Router(config)#ip route 192.168.0.0 255.255.255.0 12.0.0.2

Router 3

Router(config)#hostname r3

Router(config)#int fa0/0

Router(config)#ip add 192.168.0.1 255.255.255.0

Router(config)#no shut

Router(config)#int s0/0/0

Router(config)#ip add 12.0.0.2 255.0.0.0

Router(config)#no shut

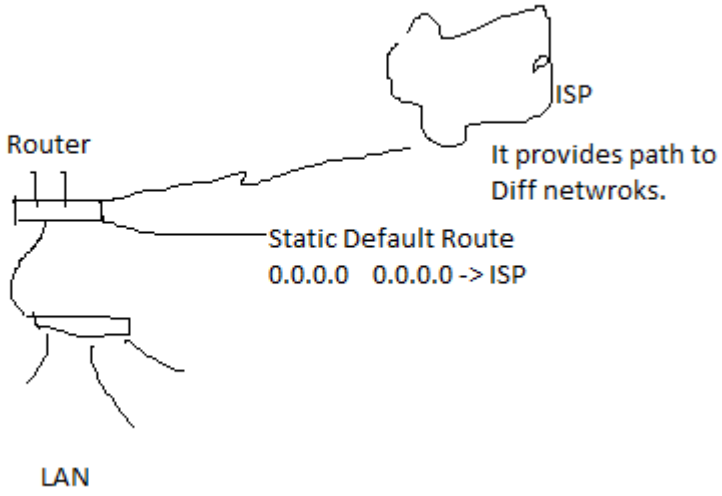
Router(config)#ip route 10.0.0.0 255.0.0.0 12.0.0.1

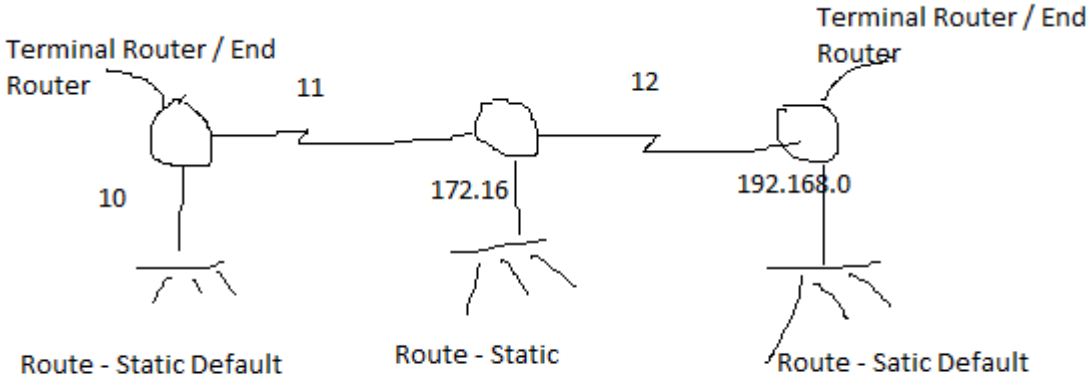
Router(config)#ip route 172.16.0.0 255.255.0.0 12.0.0.1

Router(config)#ip route 11.0.0.0 255.0.0.0 12.0.0.1

Static Default Routing

In this routing, a single route is defined at the terminal router that represents path for all destination networks with next hop router address. It is mostly used in case of connectivity with ISP.





Router 1

```
Router(config)#hostname r1
Router(config)#int fa0/0
Router(config)#ip add 10.0.0.1 255.0.0.0
Router(config)#no shut
Router(config)#int s0/0/0
Router(config)#ip add 11.0.0.1 255.0.0.0
Router(config)#clock rate 64000
Router(config)#no shut
Router(config)#ip route 12.0.0.0 255.0.0.0 11.0.0.2
Router(config)#ip route 172.16.0.0 255.255.0.0 11.0.0.2
Router(config)#ip route 192.168.0.0 255.255.255.0 11.0.0.2
Router(config)#ip route 0.0.0.0 0.0.0.0 11.0.0.2
```

Router 2

```
Router(config)#hostname r2
Router(config)#int fa0/0
Router(config)#ip add 172.16.0.1 255.255.0.0
Router(config)#no shut
Router(config)#int s0/0/0
Router(config)#ip add 11.0.0.2 255.0.0.0
Router(config)#no shut
Router(config)#int s0/0/1
Router(config)#ip add 12.0.0.1 255.0.0.0
Router(config)#clock rate 64000
Router(config)#no shut
Router(config)#ip route 10.0.0.0 255.0.0.0 11.0.0.1
Router(config)#ip route 192.168.0.0 255.255.255.0 12.0.0.2
```

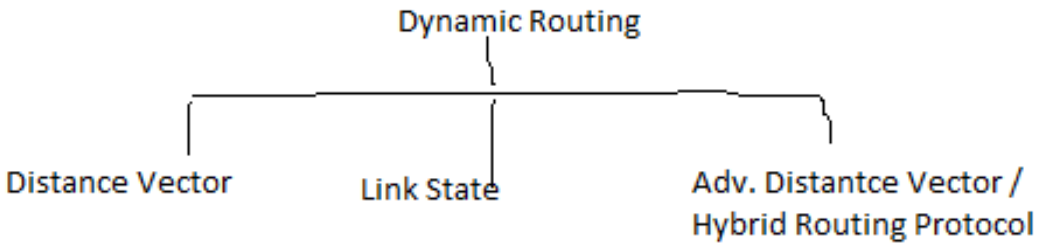
Router 3

```
Router(config)#hostname r3
Router(config)#int fa0/0
```

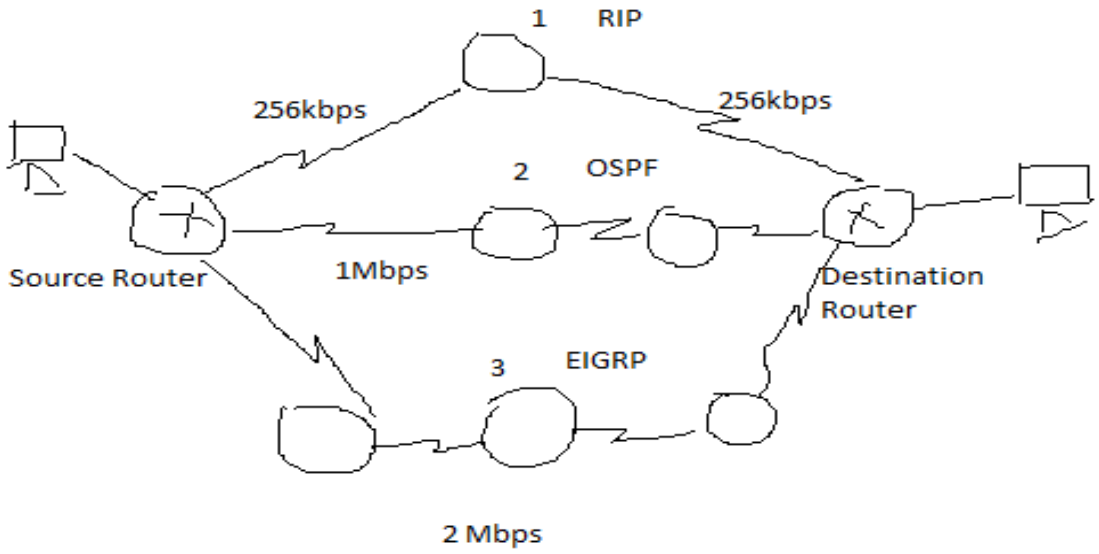
```
Router(config)#ip add 192.168.0.1 255.255.255.0
Router(config)#no shut
Router(config)#int s0/0/0
Router(config)#ip add 12.0.0.2 255.0.0.0
Router(config)#no shut
Router(config)#ip route 10.0.0.0 255.0.0.0 12.0.0.1
Router(config)#ip route 172.16.0.0 255.255.0.0 12.0.0.1
Router(config)#ip route 11.0.0.0 255.0.0.0 12.0.0.1
```

Dynamic Routing

In this routing, routes are generated and updated automatically with the help of routing protocols.



Metric:



1. Hops
2. Bandwidth
3. Delay
4. Reliability
5. MTU
6. Load

Administrative Distance (AD)-

All routing method or protocols have a numeric value by which routes can be priorities .
Value - > 0 -255
Connected routes - 0
Static route – 1
EIGRP – 90
OSPF – 110
RIP – 120
BGP - 25
Unknown route - 255

Distance Vector Routing

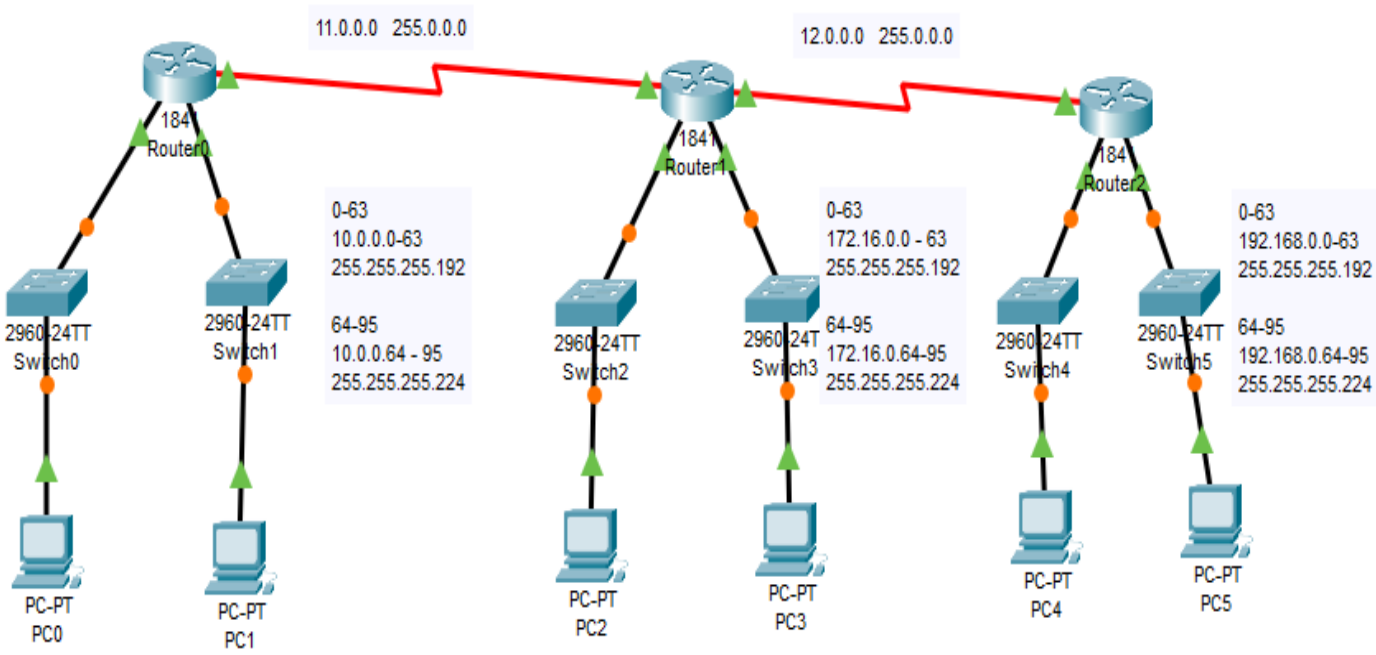
1. Metric – Hops
2. Used for small network
3. Routing by rumor (Broadcast Based)
4. Updates are sent at fixed interval of time.

5. Ex – RIP, BGP

RIP (Routing Information Protocol)

1. Distance Vector
2. Supports maximum 15 hops
3. Belmon Ford
4. Types :
   a. **RIP version 1**
      Works on broadcasting – 255.255.255.255 -> To send updates
      Updates are sent at every 30 seconds.
      Route invalid timer – 180 seconds
      Route Flush Timer – 240 seconds
      Supports class full ipv4 addressing
      Does not support auto summarization of routes.
      Configuration of RIP
      R1
      R1(config)#router rip
      Network 10.0.0.0
      Network 11.0.0.0
      R2(config)#router rip
      Network 172.16.0.0
      Network 12.0.0.0
      Network 11.0.0.0
      R3(config)#router rip
      Network 192.168.0.0
      Network 12.0.0.0

   b. RIP version 2
      Works on multicasting – 224.0.0.9 -> To send updates
      Updates are sent at every 30 seconds.
      Route invalid timer – 180 seconds
      Route Flush Timer – 240 seconds
      Supports classless (VLSM) ipv4 addressing.
      By default, it supports auto summarization of routes.



Router 1
Router(config)#router rip
Version 2
Network 10.0.0.0
Network 10.0.0.64
Network 11.0.0.0

Link State Routing :-

1. Metric – Bandwidth
2. Supports large network
3. Routing by intelligence –Triggered update
4. Sends triggered update

5. Ex – OSPF, IS-IS

OSPF (Open Shortest Path First)

1. Link State protocol
2. Open Standard
3. Metric – Bandwidth
4. Supports classless routing
5. Dijkstra Algorithm
6. Table – a. Routing Table – Best route
   Neighbor Table- Directly connected router information
7. Routing Updates – Triggered update with multicasting
8. Multicast IP – 224.0.0.5 – Receives Updates
   224.0.0.6 – Sends updates

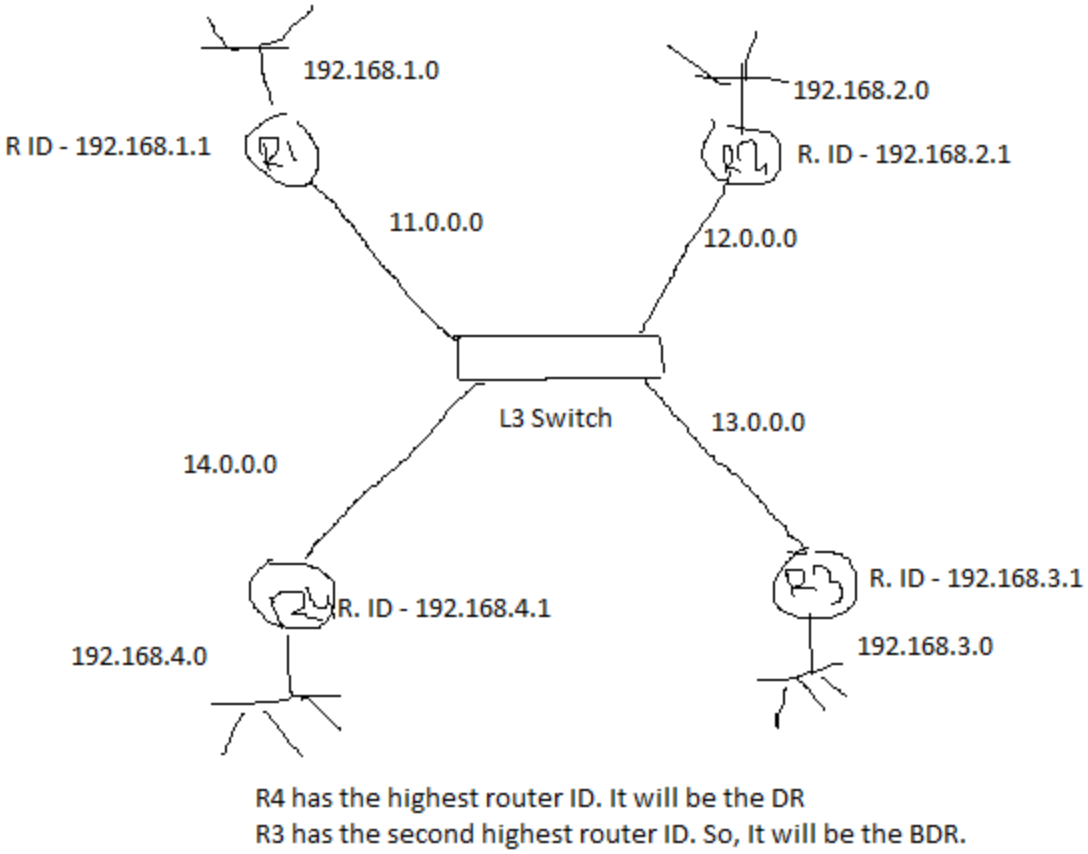
9. Router ID – It provides unique identity to each router. For ID highest IP add is used.

10. In a OSPF based network, a router with highest router ID becomes DR (Designated Router). DR receives updates from all routers and it will be responsible to forward those updates to another router.

DR will use 224.0.0.5 to receive updates.

DR will use 224.0.0.6 to send updates.

11. BDR (Backup Designated Router) – It will perform the task as DR but whenever DR will not work.



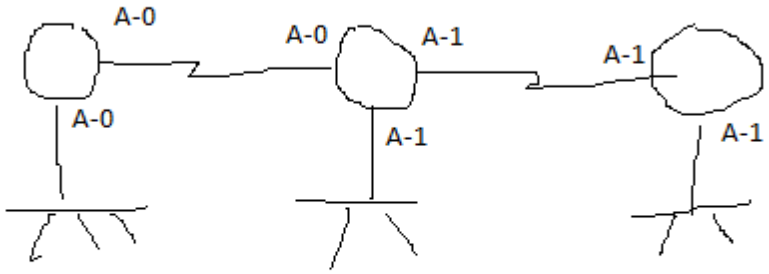
11. Area – It is a numeric value (0 – 4.2 million) that is used to divide a large OSPF based network into small part.

Area 0 is known as backbone area means all another area should be connected to area 0.

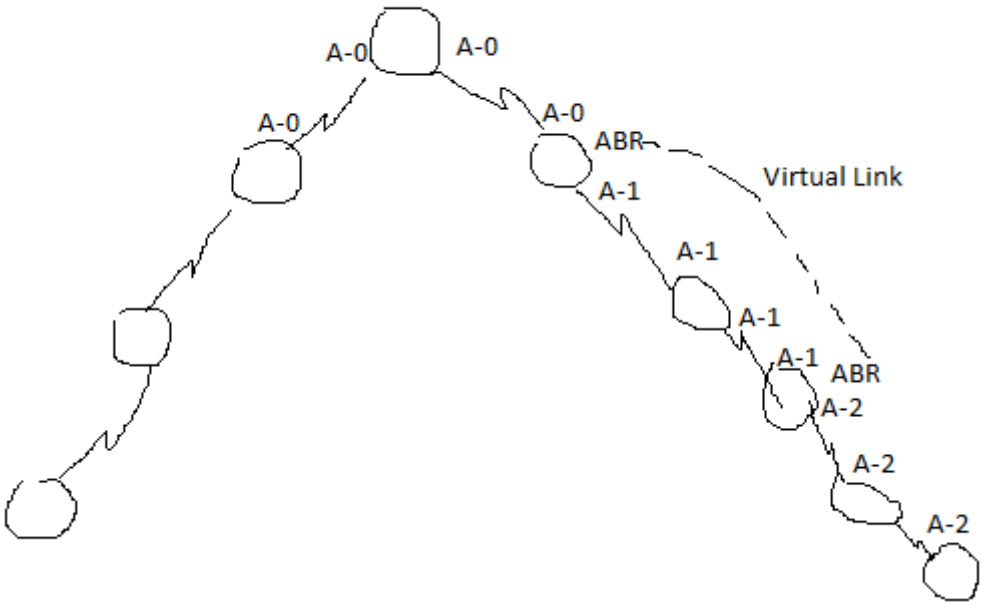
Stub Area – The last most area is known as stub area .

Area Border router (ABR) – A router which is responsible to establish connection between two or more different area.

Area Border Router (ABR)



Arera Explation



12. OSPF uses HELLO protocol to establish link between routers.
13. OSPF sends LSA (Link State Advertisement) for any kind of update between routers.
14. OSPF uses Process ID value for indifying processes executed at router.
    Process ID numeric range -> 0-65535

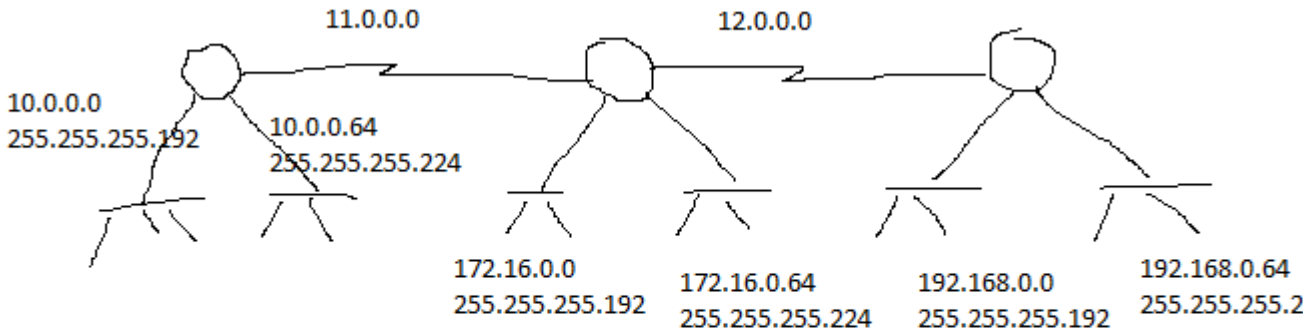
15. It uses wild card mask for abbreviation of routes (summarization of routes).

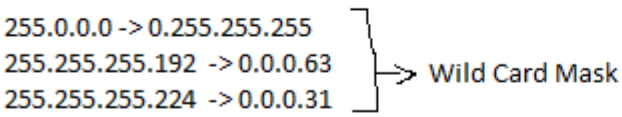
255.255.255.255
- 255.0.0.0 = 0.255.255.255
255.255.255.255
- 255.255.255.192 =0.0.0.63

255.255.255.255
- 255.255.255.224 =0.0.0.31

16. It does not support auto-summarization of routes.

Configuration of OSPF in the same area





R1(config)#router ospf 1
Net 10.0.0.0 0.0.0.63 area 0
Net 10.0.0.64 0.0.0.31 area 0
Net 11.0.0.0 0.255.255.255 area 0

R2(config)#router ospf 2
Net 172.16.0.0 0.0.0.63 area 0
Net 172.16.0.64 0.0.0.31 area 0
Net 11.0.0.0 0.255.255.255 area 0
Net 12.0.0.0 0.255.255.255 area 0

R3(config)#router ospf 3
Net 192.168.0.0 0.0.0.63 area 0
Net 192.168.0.64 0.0.0.31 area 0
Net 12.0.0.0 0.255.255.255 area 0

Configuration of OSPF with ABR

R1(config)#router ospf 1
Net 10.0.0.0 0.0.0.63 area 0
Net 10.0.0.64 0.0.0.31 area 0
Net 11.0.0.0 0.255.255.255 area 0

R2(config)#router ospf 2
Net 172.16.0.0 0.0.0.63 area 0
Net 172.16.0.64 0.0.0.31 area 1
Net 11.0.0.0 0.255.255.255 area 0
Net 12.0.0.0 0.255.255.255 area 1

R3(config)#router ospf 3
Net 192.168.0.0 0.0.0.63 area 1
Net 192.168.0.64 0.0.0.31 area 1
Net 12.0.0.0 0.255.255.255 area 1

EIGRP (Enhanced Interior Gateway Protocol)

1. Cisco proprietary – So, it can be used at Cisco devices.
2. Supports classless routing
3. Supports auto-sumrization of routes
4. Metrics : hops, bandwidth, load, MTU, delay
5. Supports maximum 255 hops
6. EIGRP supports load balancing up to 16 routes.
7. AS (Autonomous System)- 1- 65535
   This value is used for grouping or EIGRP configured routers. Routers in single AS can communicate to each other.
8. Supports large network
9. It uses HELLO protocol for link establishment.

10. Tables : Routing Table, Neighbor Table, Topology Table
11. Network down time is very less.
12. Wild card mask can be used for manual sumrization of routes.
13. Sends triggered update and sends full routing table update at every 90 minutes.
14. EIGRP is hybrid routing protocol.
15. It works on DUAL (Defusing Update Algorithum)
16. It works on multicasting – 224.0.0.10

Configuration of EIGRP :

R1(config)#router eigrp 5

#net 11.0.0.0

#net 10.0.0.0

#net 10.0.0.64

#net 10.0.0.0 0.0.0.255 -> Manual Sumrization

R2(config)#router eigrp 5

#net 11.0.0.0

#net 12.0.0.0

#net 172.16.0.0

#net 172.16.0.64

R3(config)#router eigrp 5

net 12.0.0.0

#net 192.168.0.0

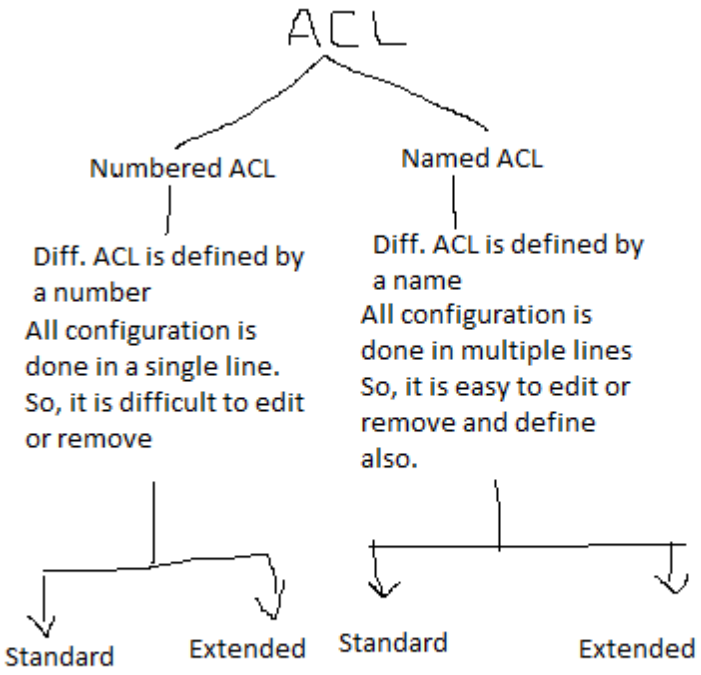
#net 192.168.0.64

Access Control List (ACL):-

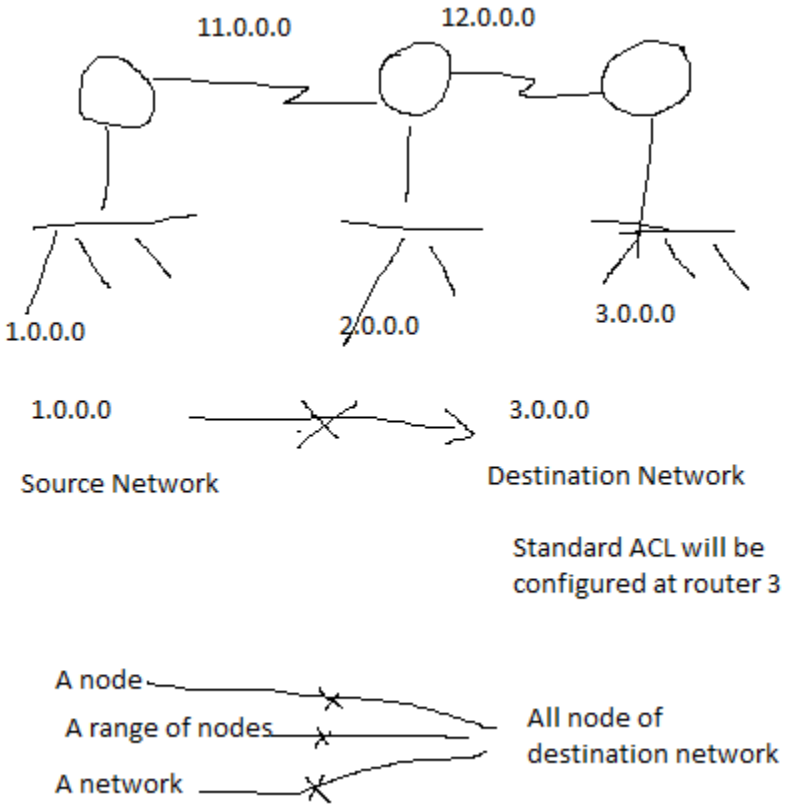
It is used to allow or deny a host or a network to communicate with another host or network. It can allow or deny all services or specific service.

So, it is known as Data Packet Filtering.
It works on IP address and services.
Telnet – 23
HTTP – 80
HTTPs – 443
DNS – 53
SSH - 22

Types of ACL :



1. Standard ACL :
   a. It uses only source address.
   b. It is always configured and implemented at destination router.
   c. For Numbered ACL –
      1 – 99, 1300 – 1999
   d. It always allow or deny all services.
   e. It always allow or deny communication from whole destination network.



Destination Router – R3

Standard ACL - Numbered

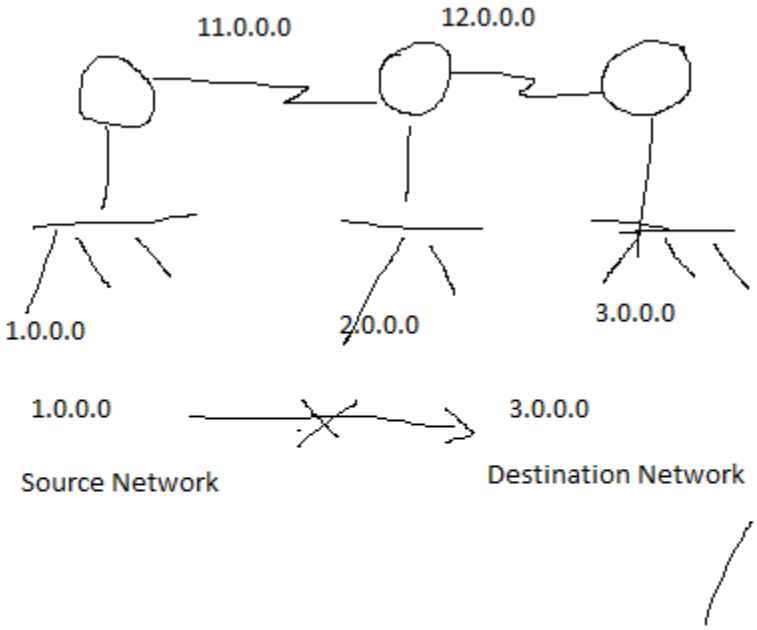
R3(config)# access-list 1 deny host 1.0.0.2
OR Access-list 1 deny 1.0.0.0 0.255.255.255
R3(config)# access-list 1 permit any
R3(config)#exit
R3(config)#int fa0/0
R3(config)#ip access-group 1 out

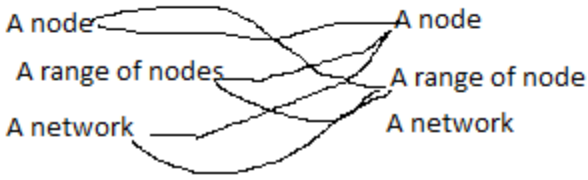
Standard ACL- Named

R3(config)#ip access-list standard motihari
R3(config)#deny host 1.0.0.2
OR #deny 1.0.0.0 0.255.255.255
R3(config)#permit any
R3(config)#exit
R3(config)#int fa0/0
R3(config)#ip access-group motihari out

Extended ACL :-

1. It uses both source and destination address.
2. It can be configured and implemented at source router.
3. Numeric Range - > 100-199, 2000-2699
4. It can allow or deny specific service or all services.
5. It can filter data packet from specific source to specific destination.





Configuration of extended ACL :

1. Configure telnet service at router 3
   R3(config)#enable password 123
   R3(config)#line vty 0
   R3(config)#password 456
   R3(config)#login
   R3(config)#exit
2. Access router 3 from any node of router 1 local network.
   PC1>telnet 12.0.0.2
   Successful ------
3. Now configure Extended ACL at router 1.

Numeric Extended ACL :
R1(config)#access-list 100 deny tcp host 1.0.0.2 host 12.0.0.2 eq 23
R1(config)#access-list 100 permit ip any any
R1(config)#int fa0/0
R1(config)#ip access-group 100 in

Named Extended ACL :-

R1(config)#ip access-list extended Dhaka
R1(config)#deny tcp host 1.0.0.2 host 12.0.0.2 eq 23
R1(config)#permit ip any any
R1(config)#exit
R1(config)#int fa0/0
R1(config)#ip access-group Dhaka in

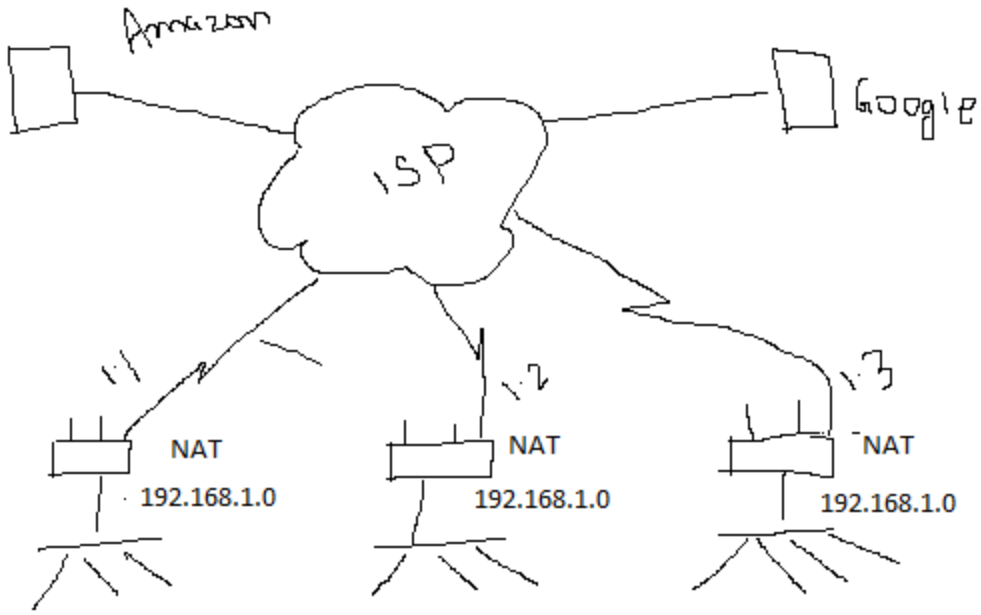
Now, to stop all source node to access router 3 through telnet :
R1(config)#access-list 101 deny tcp 1.0.0.0 0.255.255.255 host 12.0.0.2 eq 23
R1(config)#access-list 101 permit ip any any
R1(config)#exit
R1(config)#int fa0/0
R1(config)#ip access-group 101 in

Now, to stop few source nodes to access router 3 through telnet :
Range of 4 node :
Subnetmask : 255.255.255.252
Network – 0-3, 4-7, 8-11, 12-15
Wild Card Mask – 0.0.0.3
255.255.255.252
255.255.255.255
Output – 0.0.0.3

R1(config)#access-list 102 deny tcp 1.0.0.4 0.0.0.3 host 12.0.0.2 eq 23
R1(config)#access-list 102 permit ip any any
R1(config)#int fa0/0
R1(config)#ip access-group 101 in

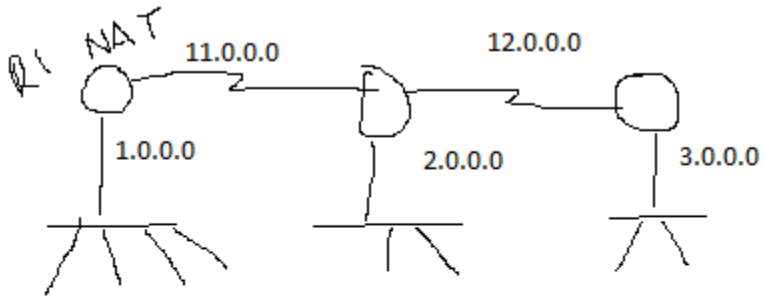
NAT (Network Address Translation)

1. It is used to convert inside local IP address into outside global IP address.
2. It increases security in the network.
3. It conserves IP address by using same ip for different network.



Types of NAT :

1. Static NAT – In this type, each inside local IP add is translated into separate outside global ip address. This translation is done manually. But, in this case only security is increased, there is no ip conservation.
2. Dynamic NAT – In this type, each inside local ip add is translated into separate outside global ip add with the help of ACL and a range of outside globalip add (pool). It increases security but there is no saving.
3. PAT (Port Address Translation): - In this type, all inside local ip add are translated into single outside ip address with the help of ACL and pool. It uses port number (1- 65535). It increases security and saves ip address.



Interface - fa0/0 -> connects inside network
s0/0/0 -> connects outside network

Dynamic NAT - local network -> 1.0.0.0 translate into 11.0.0.2 -11.0.0.100

ACL Pool

Static NAT Configuration :

R1(config)#ipnat inside source static 1.0.0.2 11.0.0.3
R1(config)#ipnat inside source static 1.0.0.3 11.0.0.4
R1(config)#int fa0/0
R1(config)#ipnat inside
R1(config)#int s0/0/0
R1(config)#ipnat outside

Dynamic NAT Configuration :-

R1(config)#access-list 1 permit 1.0.0.0 0.255.255.255
R1(config)#ipnat pool pappu 11.0.0.3 11.0.0.100 netmask 255.0.0.0
R1(config)#ipnat inside source list 1 pool pappu
R1(config)#int fa0/0
R1(config)#ipnat inside
R1(config)#int s0/0/0
R1(config)#ipnat outside

PAT (Port Address Translation) / NAT Overload

R1(config)#access-list 1 permit 1.0.0.0 0.255.255.255
R1(config)#ipnat pool pappu 11.0.0.3 11.0.0.3 netmask 255.0.0.0

```
R1(config)#ipnat inside source list 1 pool pappu overload
R1(config)#int fa0/0
R1(config)#ipnat inside
R1(config)#int s0/0/0
R1(config)#ipnat outside
```

DHCP (Dynamic Host Configuration Protocol)

This is an Application Layer protocol.
It is used to provide IP address, Subnetmask, Defaulty Gateway, DNS server address, Lease time and DHCP server address to different client nodes in a network.
All above are configured into a scope.

Configuration of DHCP at a router :

```
R1(config)#int fa0/0
R1(config)#ip add 1.0.0.1 255.0.0.0
R1(config)#no shut
R1(config)#exit
R1(config)#ipdhcp pool Bihar
R1(config)#network 1.0.0.0 255.0.0.0
R1(config)#default-router 1.0.0.1
R1(config)#dns-server 1.0.0.100
R1(config)#exit
```

NTP (Network Time Protocol)

This protocol is used for time management at different devices in the network. It synchronises time at all devices as per the configuration at NTP server. It is required for security reason and communication between server and client.

********** Switching**********

Switch :-

1. Layer 2 device and it works on Layer 3 also.
2. Layer 2 switch works on MAC address
3. Layer 3 switch works on IP address.
4. It has RJ-45 ports – RJ-45 ports are with 8 pins and SAP ports
   RJ – 11 ports are with 4 pins only
5. Switch has 4/8/16/24/48/96/128 RJ-45 ports.
6. RJ-45 ports – PoE (Power On Ethernet)
7. Port Speed – 10Mbps / 100Mbps / 1000Mbps /10G
8. It create MAC Table – L2 switch
9. Creates Routing Table – L3 switch

L2 Switch:-

1. Cisco Switches : Types : a. Unmanageable Switch

   b. Manageable Switch

2. Switch Can be configured for – VLAN, port security, speed control, Server-Client ,

3. Remote Accessing – Telnet, SSH

4. Password Security

External Part of Switch :

1. Network Port (RJ-45)
2. Uplink Port – A port with higher speed
3. Console Port – Switch Configuration

Internal Part of Switch :

1. Mother Board
2. Processor
3. SMPS
4. ROM – Keeps BIOS

5. Flash Memory – OS file , extention name (bin)
6. NVRAM – stores saved configuration.
7. RAM

Switch Configuration Mode :

Switch>- User Execute Mode

Switch# - Previllaged Mode

Switch(config)# - Global Configuration Mode

Basic Commands :-

Switch>enable -to go into previllaged mode

Switch#sh version -to get detail information about switch

Switch# sh flash: - to see the OS file

Switch# sh startup-configuration - to see the saved configuration

Switch# sh running-configuration - to see the configuration available into RAM.

Switch# sh clock - to see date and time setting.

Switch# clock set 09:05:25 7 Apr 2020 - to set date and time

Switch# config terminal - to go into global configuration mode

Switch(config)#hostname s1 - to give a name to switch

S1(config)# int vlan 1

S1(config-if)#ip address 1.0.0.1 255.0.0.0

S1(config-if)# no shutdown

S1(config-if)# exit

To set an ip add at a switch.

S1(config)# ip default-gateway 1.0.0.100

To set default gateway at a switch. With this gateway, switch can be accessed from another network.

Remote Accessing: Accessing of a node from any node of same network or different network.

Remote Accessing Tool :-

1. Telnet – (Tele Communication Network)
   Used to access a node through command line.
   Data is transmitted into plain text mode.
   So, it is insecure transmission of data.
   Port Number – 23
   Switch(config)#enable password 123
   Notes : used to make secure our switch from accessing through an unauthorised user. But this password is also required for remote accessing.
   Switch(config)# line vty 0
   Switch(config-line)#password 456
   Switch(config-line)#login
   Switch(config-line)#exit

   Notes: Telnet can be done by user defined at switch
   Commands:
   Switch(config)#username abhi password ccna
   Switch(config)#line vty 0
   Switch(config)#login local
   Switch(config)#exit

   Now, at any node :
   Go to command prompt :
   C:> telnet <give switch ip address>
   Give telnet password – 456
   S1>enable
   Give enable password
2. SSh(Secure Shell):-
   S1(config)# Ip domain name cimage
   S1(config)#Crypto key generate RSA
   1024
   S1(config)# Enable password cisco

S1(config)# Username cisco password cisco
S1(config)# Line vty 0
S1(config)#Transport input ssh
S1(config)#Login local
S1(config)#Exit
Now, at remote machine
Go to command prompt –
Ssh –l give username ip add of switch

Password Security :-

1. S1(config)#Enable Password – Plain text mode.
2. Encrypted Enable Password
   S1(config)#enable secret <password>
3. Console Port Password :-
   S1(config)#line console 0
   S1(config-line)#password abc
   S1(config-line)#login
   S1(config-line)#exit
4. Define username & password
   #username niraj password ccie
5. Console Security with user
   #line console 0
   #login local
   #exit
   To encrypt all password :
   S1(config)#service password-encryption

VLAN (Virtual Local Area Network)

It is a technique by which multiple groups of ports or node can be created at a single physical switch.
It is done by dividing the shared link between different ports of switch.
It increases security in the network.
It reduces broadcasting and collision.
By default all ports of a switch are in VLAN 1.
Diffenent VLANs are identified by a unique number and name.
This unique number is known as VLAN ID.
VLAN ID -> 1 – 4094

VLAN 1 cannot be created and deleted.
Normal VLAN -> 2 – 1001
Reserved VLAN -> 1002 – 1005
Extended VLAN -> 1006 – 4094

Types of VLAN :
1. Static VLAN
2. Dynamic VLAN

Static VLAN : Switch ports are assigned to a predefined VLAN.
Dynamic VLAN : Nodes MAC address is assigned to a predefined VLAN with the help of VMPS (VLAN Management Policy Server)

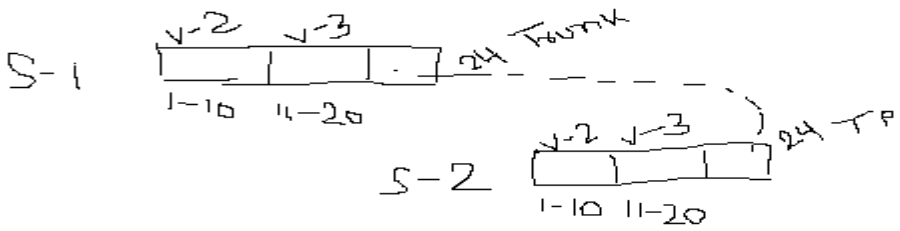
Switch Port Status (Mode) :-

1. Dynamic – in this mode switch port can change its state as per connectivity of node.
2. Access – in this mode switch port cannot change its state as per connectivity of node. It can be member of any one VLAN / it supports only one VLAN frame.
3. Trunk – in this mode switch port is not member of any VLAN. But, it supports frames of all VLAN.

Configuration of VLAN :

```
S1(config)#vlan 2
S1(config)#name sales
S1(config)#vlan 3
S1(config)#name account
S1(config)#int range fa0/1-5
S1(config)#switchport mode access
S1(config)#switchport access vlan 2
```

Trunking between switches :



It used to connect two switches to transfer data frames of different VLANs through a single port.

For this service that single port must be converted into trunk port. Trunks port is not a part of any VLAN.

Frame Tagging :

At a trunk port, VLAN ID is assigned to a each frame so that it can be identified at next switch and different VLAN frames can communicate to same VLAN.

Frame tagging Techniques :

1. dot1q – Open standard
2. ISL (Inter Switch Link) – Cisco Standard
   Configuration:

S1(config)#vlan 2

S1(config)#name sales

S1(config)#vlan 3

S1(config)#name admin

S1(config)#int range fa0/1-10

S1(config)#switchport mode access

S1(config)#switchport access vlan 2

S1(config)#int range fa0/11-20

S1(config)#switchport mode access

S1(config)#switchport access vlan 3

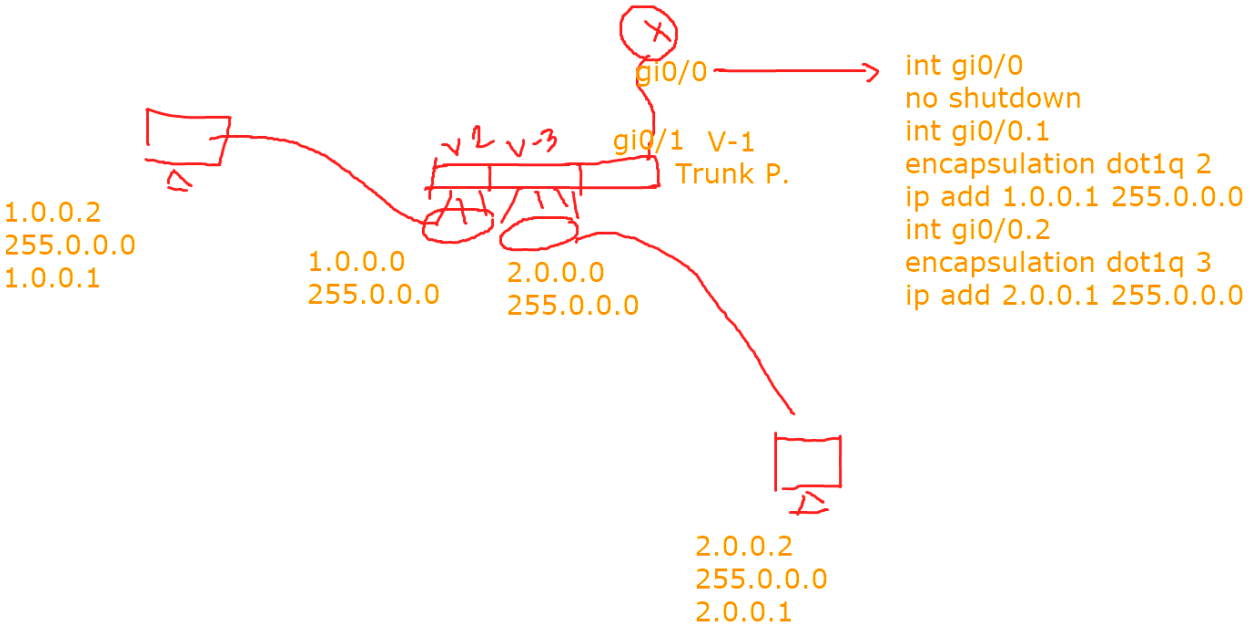
S1(config)#int gi0/1

S1(config)#switchport mode trunk

Do same configuration at next switch.

Inter VLAN Routing:

It is a process by which two or more different VLAN that are based on different subnet of IP can communicate to each other with the help of L3 device (Router / L3 switch).



Steps :

1. Create VLAN 2 and 3 at two switches.
2. Assign Port No. 1-10 to VLAN 2 and port no. 11-20 to VLAN 3 at both switches.
3. Define trunk port at s1 – fa0/23, fa0/24 & s2 – fa0/24

   S1(config)#int fa0/23
   S1(config)#switchport mode trunk
4. Now, at router use following steps :
   Router>enable
   Router#conf t
   Router(config)#hostname r1
   R1(config)#int fa0/0
   R1(config)#no shutdown
   R1(config)#int fa0/0.1
   R1(config)#encapsulation dot1q 2
   R1(config)#ip address 1.0.0.1 255.0.0.0
   R1(config)#int fa0/0.2
   R1(config)#encapsulation dot1q 3
   R1(config)#ip address 2.0.0.1 255.0.0.0
5. Now, configure default gateway at nodes connected to VLAN 2 – 1.0.0.1
6. Configure default gateway at nodes connected to VLAN 3 – 2.0.0.1

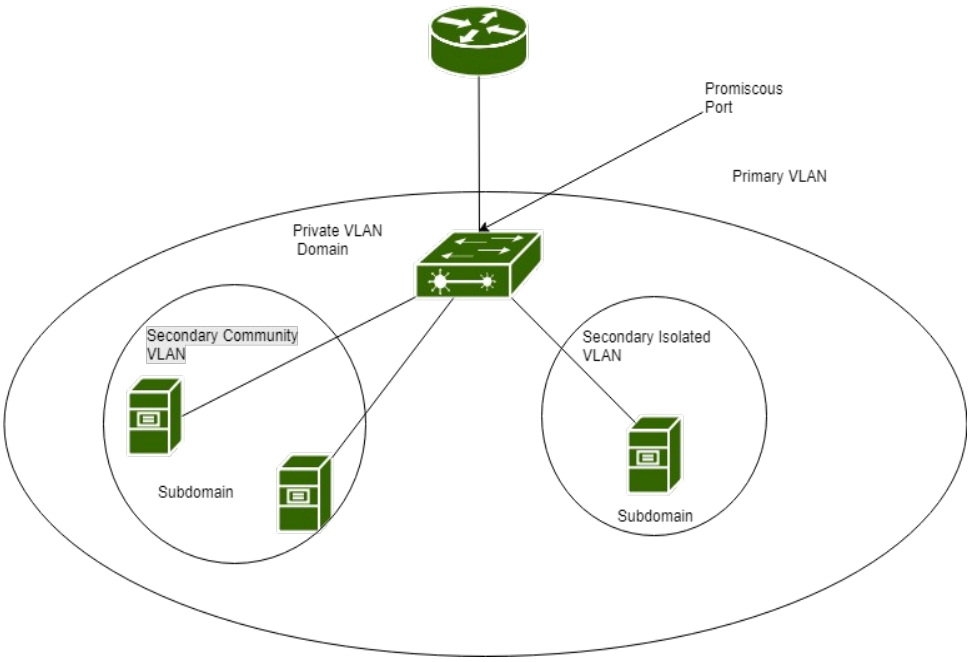
Private VLAN

Virtual LAN (VLAN) is used to break a broadcast domain into smaller domain at layer 2. Only (all) hosts belonging to same VLAN are able to communicate with each other while to communicate with other VLAN hosts, Inter Vlan routing is done. But in same VLAN, if we want some hosts should not be able to communicate with other hosts (in the same VLAN) at layer 2 level then VLAN access-list or concept of private VLAN is used.

Private VLAN –

Private VLAN are used to break the layer 2 broadcast domain into small sub-domains. A sub-domain consists of one primary VLAN and one or more secondary VLAN.

Types of VLANs –



There are two types of VLANs in Private VLANs:

1. **Primary VLAN –**
   All the ports in the private VLAN belongs to a primary VLAN. A private VLAN can have only one primary VLAN. All the VLANs in a private VLAN domain share a same primary VLAN.
2. **Secondary VLAN –**
   A private VLAN can have one or more secondary VLANs. It provides isolation between the ports belonging to same private VLAN domain. These are of two types:
   1. **Isolated VLANs –**
      Hosts belonging to Isolated VLAN can only communicate with its associated promiscuous port and cannot communicate directly with other hosts (belonging to other isolated or community VLAN) directly at layer 2. Usually a single port is assigned to Isolated VLANs but you can have more than one port associated to it.
   2. **Community VLANs –**
      A private VLAN can have one or more than one community VLANs. Hosts belonging to same community VLANs can communicate with each other and its associated promiscuous port but hosts belonging to different community VLANs cannot communicate with each other at layer 2.

Types of ports –

Types of ports in A Private VLAN are:

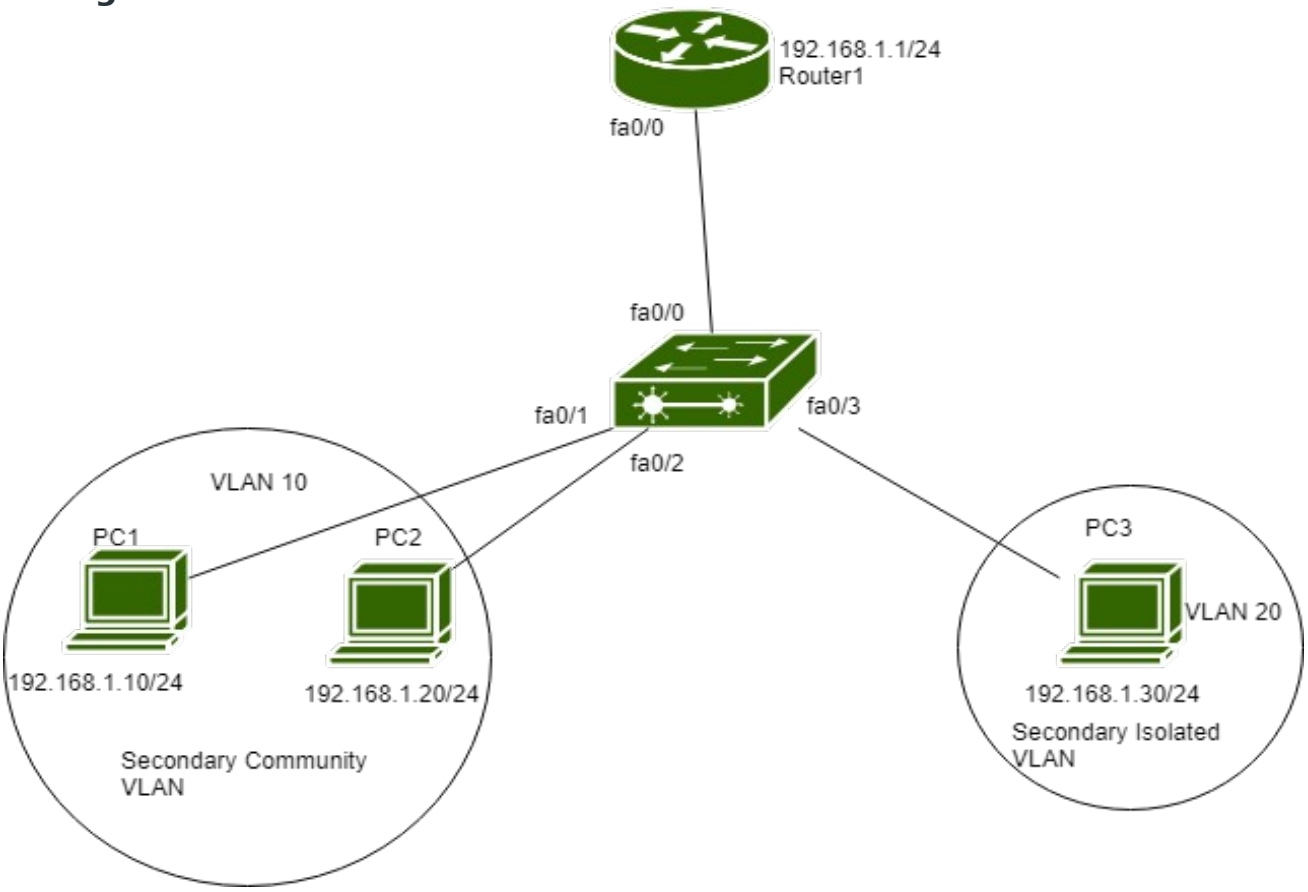
1. **Promiscuous port –**
   It belongs to the primary VLAN. These ports can communicate with all interfaces, that are a part of secondary VLANs associated with that

promiscuous port and that primary VLAN. Generally, it is used for connecting switches with routers, Firewalls etc.

2. **Isolated port –**
   An isolated port belongs to a secondary isolated VLAN.These are the host ports whose traffic is forwarded to the promiscuous port. A private VLAN allows only that traffic to the isolated port which is coming from its associated promiscuous port.
3. **Community port –**
   This port belongs to a secondary community VLAN. These host ports can communicate with other ports in the same community VLAN and also with its associated promiscuous port. These ports are completely isolated from other community VLAN ports and isolated ports.

Note –
VTP (VLAN Trunking Protocol) should be operating in mode transparent or off in order to configure private VLANs.

Configuration –



Here is a topology in which Router1 (IP address- 192.168.1.1/24), PC1(IP address- 192.168.1.10/24), PC2(IP address- 192.168.1.20/24), PC3 (IP address- 192.168.1.30/24) and switch are connected to each other as shown in the figure.
In this task, we will assign VLAN 10 to fa0/1, fa0/2 and VLAN 20 to fa0/3 and

fa0/0 as VLAN 100.Then, we will make VLAN 10 as community VLAN, VLAN 20 as isolated VLAN and VLAN 100 as primary VLAN.

Configuring Private VLAN on switch:

```
switch(config)#vlan 10
switch(config-vlan)#private-vlan community
switch(config-vlan)#exit
```

Here, we have created VLAN 10 and configured it as community VLAN. Now, configuring isolated VLAN.

```
switch(config)#vlan 20
switch(config-vlan)#private-vlan isolated
switch(config-vlan)#exit
```

Now, creating vlan 100 and configuring it as primary VLAN and associating secondary vlan 10, 20 to it.

```
switch(config)#vlan 100
switch(config-vlan)#private-vlan primary
switch(config-vlan)#private-vlan association 10, 20
switch(config-vlan)#exit
```

Now, configuring ports as private-vlan host port and associate it with primary and secondary VLAN. First configuring fa0/1 and fa0/2 and associating vlan 10 (secondary VLAN) with its primary VLAN (vlan 100).

```
switch(config)#int range fa0/1-2
switch(config-vlan)#switchport mode private-vlan host
switch(config-vlan)#switchport Private-vlan host-association 100 10
```

Now, configuring fa0/3 and associating vlan 20 (secondary VLAN) with its primary VLAN (vlan 100).

```
switch(config)#int fa0/3
switch(config-vlan)#switchport mode private-vlan host
```

```
switch(config-vlan)#switchport Private-vlan host-association 100 20
```

Now, at last we will configure interface fa0/0 as promiscuous port and associate the port with primary vlan (vlan 100) and secondary VLAN (vlan 10, 20).

```
switch(config)#int fa0/24
switch(config-vlan)#switchport mode private-vlan promiscuous
switch(config-vlan)#switchport Private-vlan mapping 100 10, 20
```

We can verify the ports associated with secondary VLANs by command.

```
switch#show vlan private-vlan
```

If you want to verify the primary VLAN and secondary VLAN (Isolated or Community) then use the command.

```
switch# show vlan private-vlan type
```

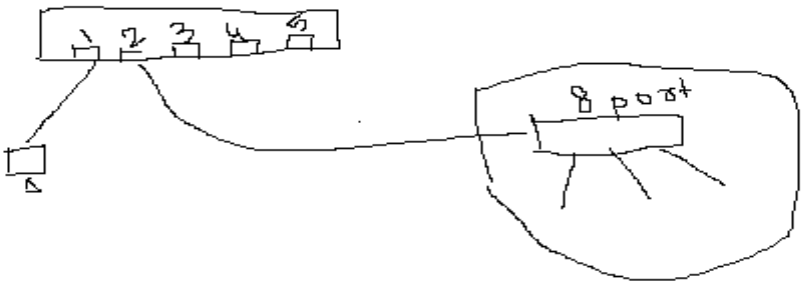
Security on Switch:

Make a MAC address static into MAC Table

S1(config)#mac address-table static <MAC address> interface fa0/24 vlan 1

Switch Port Security :-

Switch port Security is used to restrict number of nodes at a port.



S1(config)# int fa0/3

S1(config)#switchport mode access

S1(config)#switchport port-security

S1(config)#switchport port-security mac address sticky

S1(config)#switchport port-security maximum 3

S1(config)#switchport port-security violation shutdown

Switching Loop :-

BPDU – (Bridge Protocol Data Unit)

When two or more switches communicate to each other, they sends a message frame for update. It is the responsibility of each switch to send update to all another switches. It is done by BPDU.

It may cause of switching loop.

STP – Spanning Tree Protocol

This protocol by default works at switch. It is responsible to remove switching loop by blocking that port of switch through which loop occour.

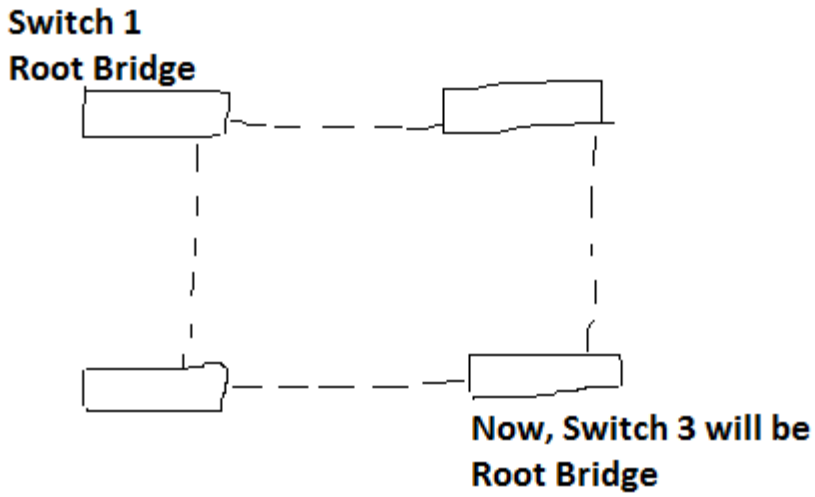
Different state of switch port :

Whenever a node is connected to a switch port, it crosses to different states :

1. Listening State – It check the physical connectivity of node and port status.
2. Learning State – It reads the MAC address of connected node and keeps this address into MAC table. It generates broadcast message. Broadcast MAC address -> FFFF-FFFF-FFFF
3. Forwarding State – In this state, switch support data transmission through a port.
4. Blocking State – Whenever, a port generates switching loop, responsible port can be in blocking state.
5. Disable State – Switch port is completely down. It can be up manually.

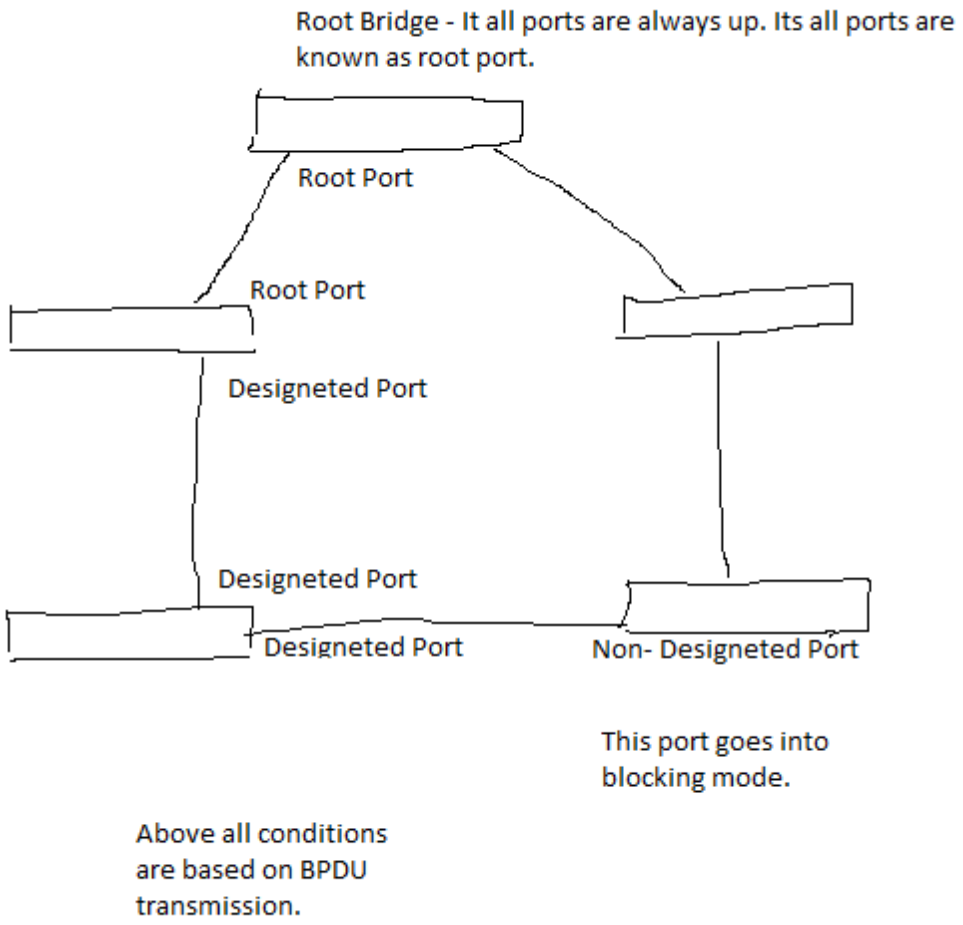
Few concepts, related to Switch Bridging :

How to change root bridge switch in a network?



Every Switch has a priority value.
Lower value higher priority
Means lowest priority value
switch will be root bridge

Switch(config)#spanning-tree vlan 1 priority 0



Spanning Tree Configuration

In this section, you will learn how to implement PVST+ and Rapid PVST+ in a switched LAN environment.

PVST+ Configuration

The focus of this topic is on how to configure PVST+ in a switched LAN environment.

Catalyst 2960 Default Configuration

Table shows the default spanning-tree configuration for a Cisco Catalyst 2960 Series switch. Notice that the default spanning-tree mode is PVST+.

Feature	Default Setting
Enable state	Enabled on VLAN 1
Spanning-tree mode	PVST+ (Rapid PVST+ and MSTP are disabled.)
Switch priority	32768
Spanning-tree port priority (configurable on a per-interface basis)	128

Configuring and Verifying the Bridge ID

When an administrator wants a specific switch to become a root bridge, the bridge priority value must be adjusted to ensure that it is lower than the bridge priority values of all the other switches on the network. There are two different methods to configure the bridge priority value on a Cisco Catalyst switch.

Method 1

To ensure that a switch has the lowest bridge priority value, use the **spanning-tree vlan** *vlan-id* **root primary** command in global configuration mode. The priority for the switch is set to the predefined value of 24,576 or to the highest multiple of 4096 less than the lowest bridge priority detected on the network.

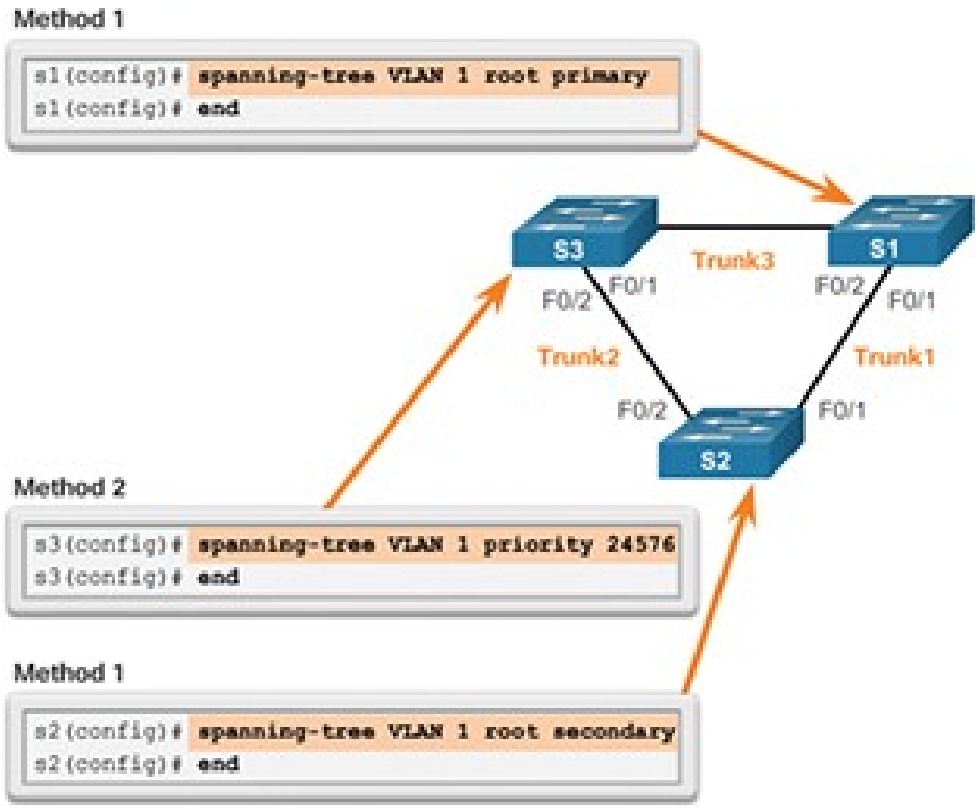
If an alternate root bridge is desired, use the **spanning-tree vlan** *vlan-id* **root secondary** global configuration mode command. This command sets the priority for the switch to the predefined value 28,672. This ensures that the alternate switch becomes the root bridge if the primary root bridge fails. This assumes that the rest of the switches in the network have the default 32,768 priority value defined.

In Figure 3-39, S1 has been assigned as the primary root bridge, using the **spanning-tree vlan 1 root primary** command, and S2 has been configured as the secondary root bridge, using the **spanning-tree vlan 1 root secondary** command.

Method 2

Another method for configuring the bridge priority value is by using the **spanning-tree vlan** *vlan-id* **priority** *value* global configuration mode command. This command gives more granular control over the bridge priority value. The priority value is configured in increments of 4096 between 0 and 61,440.

In the example in Figure 3-39, S3 has been assigned a bridge priority value of 24,576, using the **spanning-tree vlan 1 priority 24576** command.



To verify the bridge priority of a switch, use the **show spanning-tree** command. In Example 3-4, the priority of the switch has been set to 24,576. Also notice that the switch is designated as the root bridge for the spanning-tree instance.

```
S3# show spanning-tree
VLAN0001
  Spanning tree enabled protocol ieee
  Root ID    Priority     24577
```

```
              Address     000A.0033.0033
              This bridge is the root
              Hello Time   2 sec  Max Age 20 sec
Forward Delay 15 sec

 Bridge ID   Priority    24577  (priority 24576 sys-
id-ext 1)
              Address     000A.0033.3333
              Hello Time  2 sec  Max Age 20 sec
Forward Delay 15 sec
              Aging Time  300
Interface           Role Sts Cost      Prio.Nbr Type
------------------- ---- --- --------- --------
------------------------
Fa0/1               Desg FWD 4         128.1    P2p
Fa0/2               Desg FWD 4         128.2    P2p
```

PortFast and BPDU Guard (3.3.1.3)

PortFast is a Cisco feature for PVST+ environments. When a switch port is configured with PortFast, that port transitions from blocking to forwarding state immediately, bypassing the usual 802.1D STP transition states (the listening and learning states). As shown in Figure 3-40, you can use PortFast on access ports to allow these devices to connect to the network immediately rather than wait for IEEE 802.1D STP to converge on each VLAN. Access ports are ports that are connected to a single workstation or to a server.

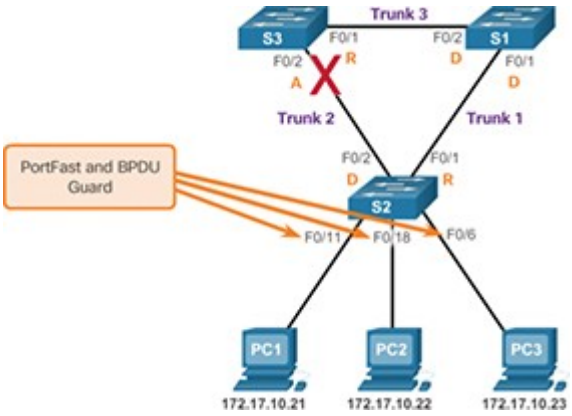


Figure 3-40 PortFast and BPDU Guard Topology

In a valid PortFast configuration, BPDUs should never be received because that would indicate that another bridge or switch is connected to the port, potentially causing a spanning-tree loop. Cisco switches support a feature called BPDU guard. When it is enabled, BPDU guard puts the port in an errdisabled (error-disabled) state on receipt of a BPDU. This effectively shuts down the port. The BPDU guard feature provides a secure response to invalid configurations because you must manually put the interface back into service.

Cisco PortFast technology is useful for DHCP. Without PortFast, a PC can send a DHCP request before the port is in forwarding state, denying the host from getting a usable IP address and other information. Because PortFast immediately changes the state to forwarding, the PC always gets a usable IP address (if the DHCP server has been configured correctly and communication with the DHCP server has occurred).

NOTE

Because the purpose of PortFast is to minimize the time that access ports must wait for spanning tree to converge, it should be used only on access ports. If you enable PortFast on a port connecting to another switch, you risk creating a spanning-tree loop.

To configure PortFast on a switch port, enter the **spanning-tree portfast** interface configuration mode command on each interface on which PortFast is to be enabled, as shown in Example 3-5.

Example 3-5 Configuring PortFast

```
S2(config)# interface FastEthernet 0/11
S2(config-if)# spanning-tree portfast
%Warning: portfast should only be enabled on ports connected to a single
   host. Connecting hubs, concentrators, switches, bridges, etc... to this
   interface when portfast is enabled, can cause temporary bridging loops.
   Use with CAUTION
```

```
%Portfast has been configured on FastEthernet0/11 but
will only
   have effect when the interface is in a non-trunking
mode.


S2(config-if)#
```

The **spanning-tree portfast default** global configuration mode command enables PortFast on all non-trunking interfaces.

To configure BPDU guard on a Layer 2 access port, use the **spanning-tree bpduguard enable** interface configuration mode command, as shown in Example 3-6.

Example 3-6 Configuring and Verifying BPDU Guard

```
S2(config-if)#  spanning-tree bpduguard enable
S2(config-if)# end
S2#
S2# show running-config interface f0/11
interface FastEthernet0/11
spanning-tree portfast
spanning-tree bpduguard enable

S2#
```

The **spanning-tree portfast bpduguard default** global configuration command enables BPDU guard on all PortFast-enabled ports.

Notice in Example 3-6 how the **show running-config interface** command can be used to verify that PortFast and BPDU guard have been enabled for a switch port. PortFast and BPDU guard are disabled, by default, on all interfaces.

PVST+ Load Balancing (3.3.1.4)

The topology in Figure 3-41 shows three switches with 802.1Q trunks connecting them.

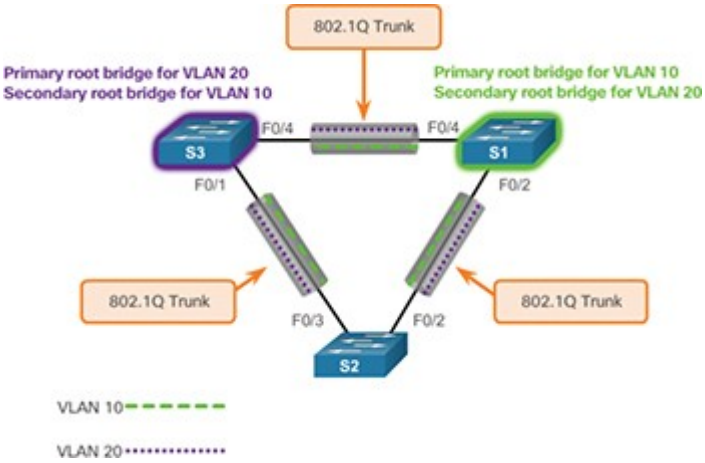


Figure 3-41 PVST+ Configuration Topology

Two VLANs, 10 and 20, are being trunked across these links. The goal is to configure S3 as the root bridge for VLAN 20 and S1 as the root bridge for VLAN 10. Port F0/3 on S2 is the forwarding port for VLAN 20 and the blocking port for VLAN 10. Port F0/2 on S2 is the forwarding port for VLAN 10 and the blocking port for VLAN 20.

In addition to establishing a root bridge, it is also possible to establish a secondary root bridge. A secondary root bridge is a switch that may become the root bridge for a VLAN if the primary root bridge fails. Assuming that the other bridges in the VLAN retain their default STP priority, this switch becomes the root bridge if the primary root bridge fails.

Configuring PVST+ on this topology involves the following steps:

- **Step 1.** Select the switches you want for the primary and secondary root bridges for each VLAN. For example, in Figure 3-41, S3 is the primary bridge for VLAN 20, and S1 is the secondary bridge for VLAN 20.

- **Step 2.** As shown in Example 3-7, configure S3 to be a primary bridge for VLAN 10 and the secondary bridge for VLAN 20 by using the **spanning-tree vlan** *number* **root** { **primary** | **secondary** } command.

Example 3-7 Configuring Primary and Secondary Root Bridges for Each VLAN on S3

```
S3(config)#  spanning-tree vlan 20 root primary
S3(config)# spanning-tree vlan 10 root secondary
```

- **Step 3.** As shown in Example 3-8, configure S1 to be a primary bridge for VLAN 20 and the secondary bridge for VLAN 10.

Example 3-8 Configuring Primary and Secondary Root Bridges for Each VLAN on S1

```
S1(config)# spanning-tree vlan 10 root primary
S1(config)# spanning-tree vlan 20 root secondary
```

Another way to specify the root bridge is to set the spanning-tree priority on each switch to the lowest value so that the switch is selected as the primary bridge for its associated VLAN, as shown in Example 3-9.

Example 3-9 Configuring the Lowest Possible Priority to Ensure That a Switch Is Root

```
S3(config)#  spanning-tree vlan 20 priority 4096
S1(config)# spanning-tree vlan 10 priority 4096
```

The switch priority can be set for any spanning-tree instance. This setting affects the likelihood that a switch is selected as the root bridge. A lower value increases the probability that the switch is selected. The range is 0 to 61,440, in increments of 4096; all other values are rejected. For example, a valid priority value is 4096 × 2 = 8192.

As shown in Example 3-10, the **show spanning-tree active** command displays spanning-tree configuration details for the active interfaces only.

The output shown is for S1 configured with PVST+. A number of Cisco IOS command parameters are associated with the **show spanning-tree** command.

In Example 3-11, the output shows that the priority for VLAN 10 is 4096, the lowest of the three respective VLAN priorities.

Example 3-10 Verifying STP Active Interfaces

```
S1#  show spanning-tree active
<output omitted>
VLAN0010
  Spanning tree enabled protocol ieee
```

```
  Root ID    Priority    4106
             Address     ec44.7631.3880
             This bridge is the root
             Hello Time   2 sec  Max Age 20 sec
Forward Delay 15 sec

   Bridge ID Priority    4106   (priority 4096 sys-id-
ext 10)
             Address     ec44.7631.3880
             Hello Time  2 sec  Max Age 20 sec
Forward Delay 15 sec
             Aging Time  300 sec

Interface           Role Sts Cost      Prio.Nbr Type
------------------- ---- --- --------- --------
--------------------------------
Fa0/3               Desg FWD 19        128.5    P2p
Fa0/4               Desg FWD 19        128.6    P2p
```

Example 3-11 Verifying the S1 STP Configuration

```
S1#  show running-config | include span
spanning-tree mode pvst
spanning-tree extend system-id
spanning-tree vlan 1 priority 24576
spanning-tree vlan 10 priority 4096
spanning-tree vlan 20 priority 28672
```

Packet Tracer 3.3.1.5: Configuring PVST+

In this activity, you will configure VLANs and trunks and examine and configure the Spanning Tree Protocol primary and secondary root bridges. You will also optimize the switched topology by using PVST+, PortFast, and BPDU guard.

Rapid PVST+ Configuration (3.3.2)

Rapid PVST+ is the Cisco implementation of RSTP. It supports RSTP on a per-VLAN basis. The focus of this topic is on how to configure Rapid PVST+ in a switched LAN environment.

Spanning Tree Mode (3.3.2.1)

Rapid PVST+ commands control the configuration of VLAN spanning-tree instances. A spanning-tree instance is created when an interface is assigned to a VLAN, and is removed when the last interface is moved to another VLAN. In addition, you can configure STP switch and port parameters before a spanning-tree instance is created. These parameters are applied when a spanning-tree instance is created.

Use the **spanning-tree mode rapid-pvst** global configuration mode command to enable Rapid PVST+. Optionally, you can also identify interswitch links as point-to-point links by using the **spanning-tree link-type point-to-point** interface configuration command. When specifying an interface to configure, valid interfaces include physical ports, VLANs, and port channels.

To reset and reconverge STP, use the **clear spanning-tree detected-protocols** privileged EXEC mode command.

To illustrate how to configure Rapid PVST+, refer to the topology in Figure 3-42.

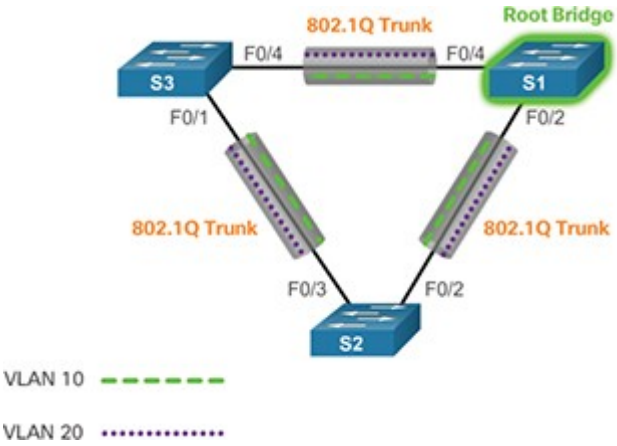


Figure 3-42 Rapid PVST+ Topology

NOTE

The default spanning-tree configuration on a Catalyst 2960 Series switch is PVST+. A Catalyst 2960 switch supports PVST+, Rapid PVST+, and MST, but only one version can be active for all VLANs at any time.

Example 3-12 displays the commands to configure Rapid PVST+ on S1.

Example 3-12 Configuring Rapid PVST+ on S1

```
S1# configure terminal
S1(config)# spanning-tree mode rapid-pvst
S1(config)# spanning-tree vlan 1 priority 24576
S1(config)# spanning-tree vlan 10 priority 4096
S1(config)# spanning-tree vlan 20 priority 28672
S1(config)# interface f0/2
S1(config-if)# spanning-tree link-type point-to-point
S1(config-if)# end
S1# clear spanning-tree detected-protocols
```

In Example 3-13, the **show spanning-tree vlan 10** command shows the spanning-tree configuration for VLAN 10 on switch S1.

Example 3-13 Verifying That VLAN 10 Is Using RSTP

```
S1# show spanning-tree vlan 10

VLAN0010
  Spanning tree enabled protocol rstp
  Root ID     Priority    4106
              Address     ec44.7631.3880
              This bridge is the root
              Hello Time  2 sec  Max Age 20 sec
Forward Delay 15 sec

  Bridge ID   Priority    4106   (priority 4096 sys-
id-ext 10)
              Address     ec44.7631.3880
              Hello Time  2 sec  Max Age 20 sec
Forward Delay 15 sec
              Aging Time  300 sec
Interface           Role Sts Cost      Prio.Nbr Type
------------------- ---- --- --------- --------
--------------------------------
Fa0/3               Desg FWD 19        128.5    P2p
Peer(STP)
Fa0/4               Desg FWD 19        128.6    P2p
Peer(STP)
```

In the output, the statement “Spanning tree enabled protocol rstp” indicates that S1 is running Rapid PVST+. Notice that the BID priority is set to 4096. Because S1 is the root bridge for VLAN 10, all of its interfaces are designated ports.

In Example 3-14, the **show running-config** command is used to verify the Rapid PVST+ configuration on S1.

Example 3-14 Verifying the Rapid PVST+ Configuration

```
S1#  show running-config | include span
spanning-tree mode rapid-pvst
spanning-tree extend system-id
spanning-tree vlan 1 priority 24576
spanning-tree vlan 10 priority 4096
spanning-tree vlan 20 priority 28672
spanning-tree link-type point-to-point
```

NOTE

Generally, it is unnecessary to configure the **point-to-point link-type** parameter for Rapid PVST+ because it is unusual to have a shared link type. In most cases, the only difference between configuring PVST+ and Rapid PVST+ is the **spanning-tree mode rapid-pvst** command.

Packet Tracer 3.3.2.2: Configuring Rapid PVST+

In this activity, you will configure VLANs and trunks and examine and configure the spanning-tree primary and secondary root bridges. You will also optimize it by using rapid PVST+, PortFast, and BPDU guard.

Lab 3.3.2.3: Configuring Rapid PVST+, PortFast, and BPDU Guard

Refer to *Scaling Networks v6 Labs & Study Guide* and the online course to complete this activity.

In this lab, you will complete the following objectives:

- Part 1: Build the Network and Configure Basic Device Settings
- Part 2: Configure VLANs, Native VLAN, and Trunks
- Part 3: Configure the Root Bridge and Examine PVST+ Convergence
- Part 4: Configure Rapid PVST+, PortFast, BPDU Guard, and Examine Convergence

STP Configuration Issues (3.3.3)

The focus of this topic is on how to analyze common STP configuration issues.

Analyzing the STP Topology (3.3.3.1)

To analyze the STP topology, follow these steps, as shown in the logic diagram in Figure 3-43:

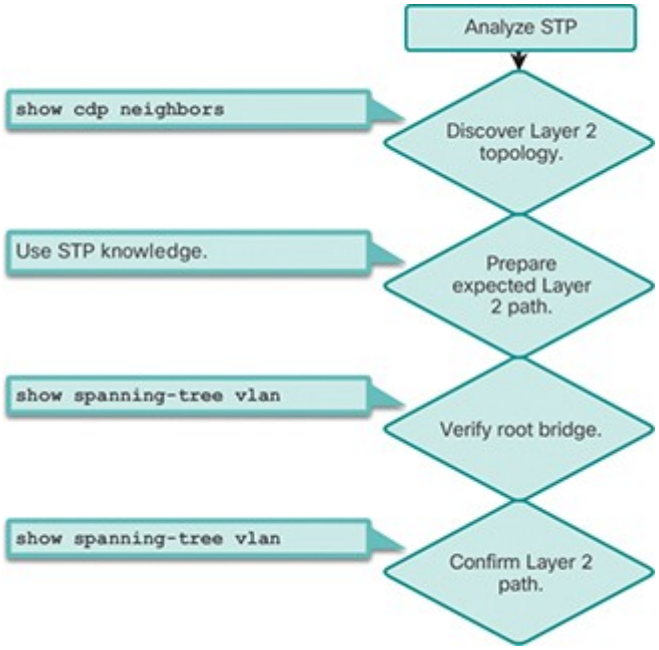


Figure 3-43 Analyzing the STP Topology

- **Step 1.** Discover the Layer 2 topology. Use network documentation if it exists or use the **show cdp neighbors** command to discover the Layer 2 topology.
- **Step 2.** After discovering the Layer 2 topology, use STP knowledge to determine the expected Layer 2 path. It is necessary to know which switch is the root bridge.
- **Step 3.** Use the **show spanning-tree vlan** command to determine which switch is the root bridge.
- **Step 4.** Use the **show spanning-tree vlan** command on all switches to find out which ports are in blocking or forwarding state and confirm your expected Layer 2 path.

Expected Topology versus Actual Topology (3.3.3.2)

In many networks, the optimal STP topology is determined as part of the network design and then implemented through manipulation of STP priority and cost values, as shown in Figure 3-44.

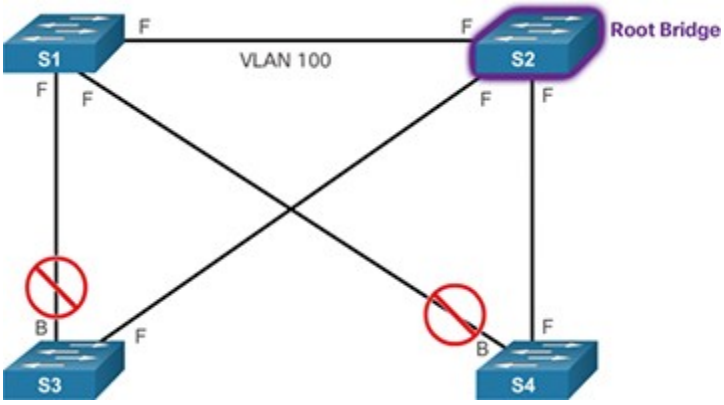


Figure 3-44 Verifying That Actual Topology Matches Expected Topology

Situations may occur in which STP was not considered in the network design and implementation, or in which it was considered or implemented before the network underwent significant growth and change. In such situations, it is important to know how to analyze the STP topology in the operational network.

A big part of troubleshooting consists of comparing the actual state of the network against the expected state of the network and spotting the differences to gather clues about the troubleshooting problem. A network professional should be able to examine the switches and determine the actual topology, as well as understand what the underlying spanning-tree topology should be.

Overview of Spanning Tree Status (3.3.3.3)

Using the **show spanning-tree** command without specifying any additional options provides a quick overview of the status of STP for all VLANs that are defined on a switch.

Use the **show spanning-tree vlan** *vlan_id* command to get STP information for a particular VLAN. Use this command to get information about the role and status of each port on the switch. If you are interested only in a particular VLAN, limit the scope of this command by specifying that VLAN as an option, as shown for VLAN 100 in Figure 3-45.

The output on switch S1 in this example shows all three ports in the forwarding (FWD) state and the roles of the three ports as either designated ports or root ports. Any ports being blocked display the output status as “BLK.”

The output also gives information about the BID of the local switch and the root ID, which is the BID of the root bridge.

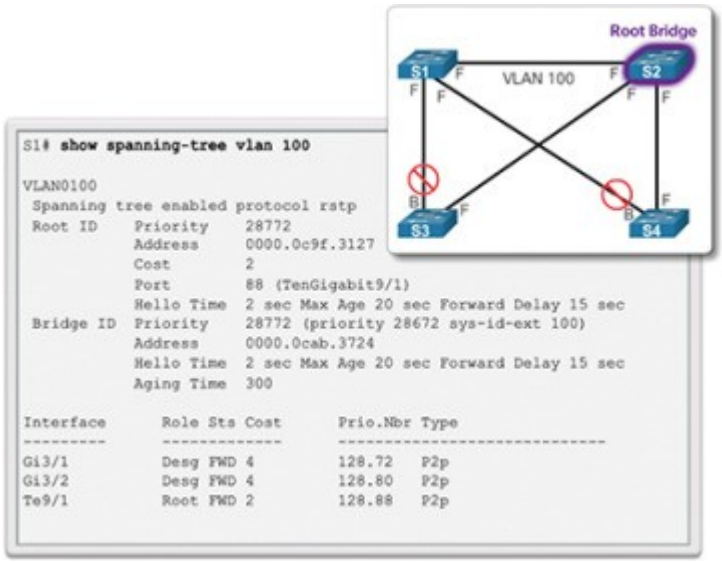


Figure 3-45 Overview of STP Status

Spanning Tree Failure Consequences (3.3.3.4)

Figure 3-46 shows a functional STP network. But what happens when there is an STP failure?

There are two types of STP failure. First, STP might erroneously block ports that should have gone into the forwarding state. Connectivity might be lost for traffic that would normally pass through this switch, but the rest of the network remains unaffected. Second, STP might erroneously move one or more ports into the forwarding state, as shown for S4 in Figure 3-47.

Remember that an Ethernet frame header does not include a TTL field, which means that any frame that enters a bridging loop continues to be forwarded by the switches indefinitely. The only

exceptions are frames that have their destination address recorded in the MAC address table of the switches. These frames are simply forwarded to the port that is associated with the MAC address and do not enter a loop. However, any frame that is flooded by a switch enters the loop. This may include broadcasts, multicasts, and unicasts with a globally unknown destination MAC address.

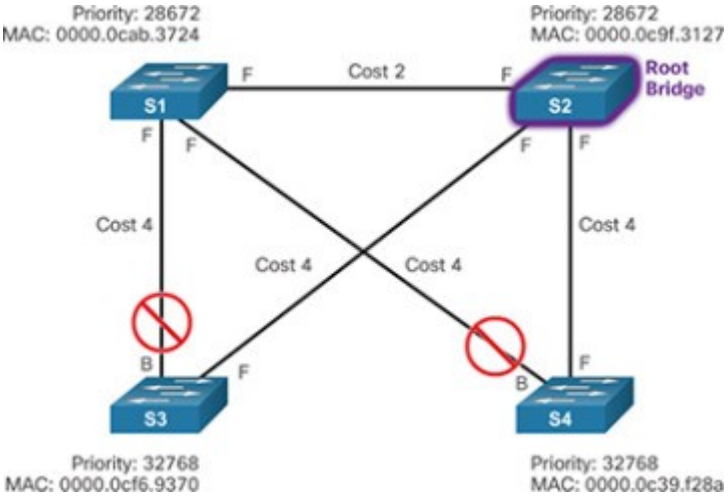


Figure 3-46 STP Switch Topology

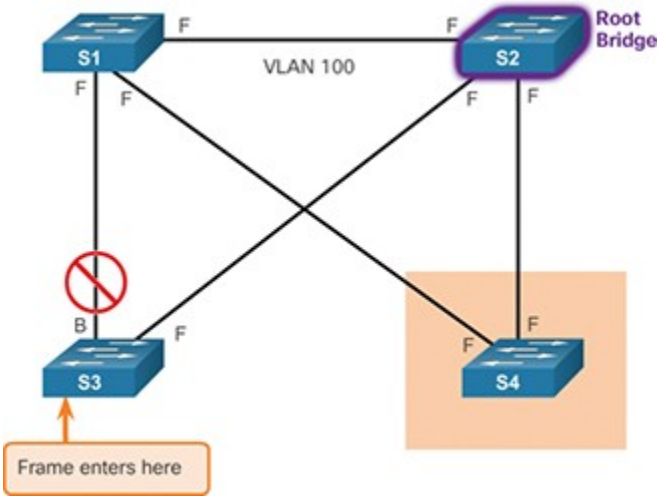


Figure 3-47 Erroneous Transition to Forwarding

Figure 3-48 shows the consequences and corresponding symptoms of STP failure.

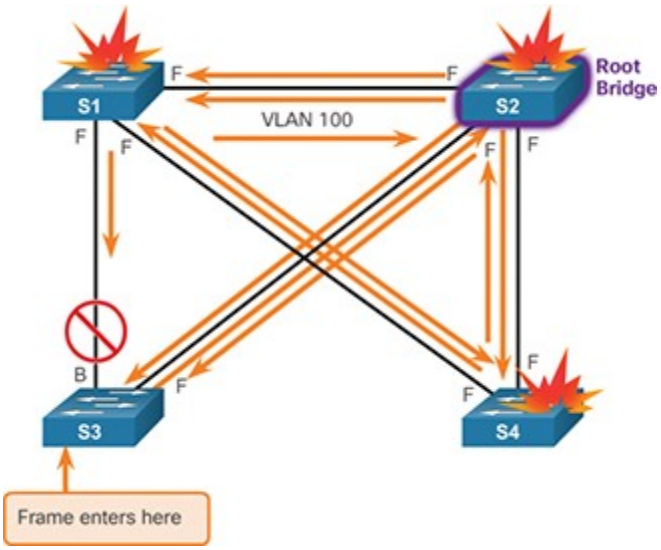


Figure 3-48 Consequences of STP Failure Are Severe

The load on all links in the switched LAN quickly starts increasing as more and more frames enter the loop. This problem is not limited to the links that form the loop but also affects any other links in the switched domain because the frames are flooded on all links. When the spanning-tree failure is limited to a single VLAN only, links in that VLAN are affected. Switches and trunks that do not carry that VLAN operate normally.

If the spanning-tree failure has created a bridging loop, traffic increases exponentially. The switches then flood the broadcasts out multiple ports. This creates copies of the frames every time the switches forward them.

When control plane traffic (for example, routing messages) starts entering the loop, the devices that are running these protocols quickly start getting overloaded. Their CPUs approach 100 percent utilization while they are trying to process an ever-increasing load of control plane traffic. In many cases, the earliest indication of this broadcast storm in progress is that routers or Layer 3 switches report control plane failures and that they are running at a high CPU load.

The switches experience frequent MAC address table changes. If a loop exists, a switch may see a frame with a certain source MAC address coming in on one port and then see another frame with

the same source MAC address coming in on a different port a fraction of a second later. This causes the switch to update the MAC address table twice for the same MAC address.

Repairing a Spanning Tree Problem (3.3.3.5)

One way to correct spanning-tree failure is to manually remove redundant links in the switched network, either physically or through configuration, until all loops are eliminated from the topology. When the loops are broken, the traffic and CPU loads should quickly drop to normal levels, and connectivity to devices should be restored.

Although this intervention restores connectivity to the network, it is not the end of the troubleshooting process. All redundancy from the switched network has been removed, and now the redundant links must be restored.

If the underlying cause of the spanning-tree failure has not been fixed, chances are that restoring the redundant links will trigger a new broadcast storm. Before restoring the redundant links, determine and correct the cause of the spanning-tree failure. Carefully monitor the network to ensure that the problem is fixed.

Activity 3.3.3.6: Troubleshoot STP Configuration Issues

Refer to the online course to complete this activity.

Switch Stacking and Chassis Aggregation (3.3.4)

The focus of this topic is to explain the value of switch stacking and chassis aggregation in a small switched LAN.

Switch Stacking Concepts (3.3.4.1)

A switch stack can consist of up to nine Catalyst 3750 switches connected through their StackWise ports. One of the switches controls the operation of the stack and is called the *stack master*. The stack master and the other switches in the stack are stack members.

Figure 3-49 shows the backplane of four Catalyst 3750 switches and how they are connected in a stack.

Every member is uniquely identified by its own stack member number. All members are eligible masters. If the master becomes unavailable, there is an automatic process to elect a new master from the remaining stack members. One of the factors is the stack member priority value. The switch with the highest stack member priority value becomes the master.

Layer 2 and Layer 3 protocols present the entire switch stack as a single entity to the network. One of the primary benefits of switch stacks is that you manage the stack through a single IP address. The IP address is a system-level setting and is not specific to the master or to any other member. You can manage the stack through the same IP address even if you remove the master or any other member from the stack.

Figure 3-49 Cisco Catalyst 3750 Switch Stack

The master contains the saved and running configuration files for the stack. Therefore, there is only one configuration file to manage and maintain. The configuration files include the system-

level settings for the stack and the interface-level settings for each member. Each member has a current copy of these files for backup purposes.

The switch is managed as a single switch, including passwords, VLANs, and interfaces. Example 3-15 shows the interfaces on a switch stack with four 52-port switches. Notice that the first number after the interface type is the stack member number.

Example 3-15 Switch Stack Interfaces

```
Switch# show running-config | begin interface
interface GigabitEthernet1/0/1
!
interface GigabitEthernet1/0/2
!
interface GigabitEthernet1/0/3
!
<output omitted>
!
interface GigabitEthernet1/0/52
!
interface GigabitEthernet2/0/1
!
interface GigabitEthernet2/0/2
!
<output omitted>
!
interface GigabitEthernet2/0/52
!
interface GigabitEthernet3/0/1
!
interface GigabitEthernet3/0/2
```

```
!
<output omitted>
!
interface GigabitEthernet3/0/52
!
interface GigabitEthernet4/0/1
!
interface GigabitEthernet4/0/2
!
<output omitted>
!
interface GigabitEthernet4/0/52
!
Switch#
```

Spanning Tree and Switch Stacks (3.3.4.2)

Another benefit to switch stacking is the ability to add more switches to a single STP instance without increasing the *STP diameter*. The diameter is the maximum number of switches that data must cross to connect any two switches. The IEEE recommends a maximum diameter of seven switches for the default STP timers. For example, in Figure 3-50, the diameter from S1-4 to S3-4 is nine switches. This design violates the IEEE recommendation.

Figure 3-50 Diameter Greater Than 7

The recommended diameter is based on default STP timer values, which are as follows:

- **Hello Timer (2 seconds)**—The interval between BPDU updates.
- **Max Age Timer (20 seconds)**—The maximum length of time a switch saves BPDU information.
- **Forward Delay Timer (15 seconds)**—The time spent in the listening and learning states.

NOTE

The formulas used to calculate the diameter are beyond the scope of this course. Refer to the following Cisco document for more information: www.cisco.com/c/en/us/support/docs/lan-switching/spanning-tree-protocol/19120-122.html.

Switch stacks help maintain or reduce the impact of diameter on STP reconvergence. In a switch stack, all switches use the same bridge ID for a given spanning-tree instance. This means that, if the switches are stacked, as shown in Figure 3-51, the maximum diameter becomes 3 instead of 9.

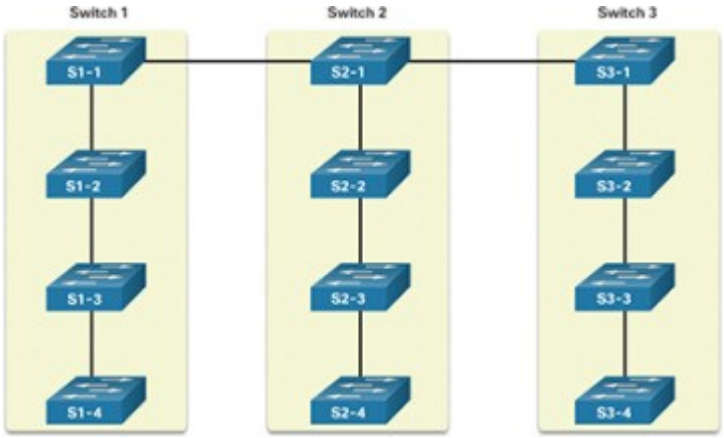


Figure 3-51 Switch Stacking Reduces STP Diameter

Ether Channel :

It is a technique to combine multiple port of a switch to link with another switch. It increases bandwidth and provides fault tolerance in the network. Switching loop is not generated between two switches because switch port are combined under a logical interface.

It is done by Channel Group. Maximum 6 channel groups can be created a physical switch. In case of Multiple channel group only one group is active while another groups logical interface are in disable state as per rule of STP. Ether channel is also used for load balancing.

Ether Channel Group is based on two techniques:

1. PAGP – Mode -> auto, desirable
2. LACP - Mode -> active, passive

Before creating the channel-group with switch ports, ports must be in trunking mode because trunk port supports frames of all VLANs and it is not member of any VLAN.

Steps:

S1(config)#int range fa0/22-24

S1(config)#switchport mode trunk

S1(config)#channel-group 1 mode auto

S2(config)#int range fa0/22-24

S2(config)#switchport mode trunk

S2(config)#channel-group 1 mode desirable

Router Password Recovery :-

Enable Password Setting:

R1(config)#enable password 123

R1(config)#enable secret 456 --→ It is encrypted password with higher priority.

Console Port Password:

R1(config)#line con 0

R1(config)#password 789

R1(config)#login

R1(config)#exit

How to save password?

R1# write memory

Recovery of password:

Router IOS – Flash Memory

Router Saved configuration – NVRAM – Register Value – 0x2102

Router Running Configuration – RAM

Booting Process –

Power On -> ROM (BIOS) -> Flash Memory (IOS) -> RAM -> Booting

NVRAM(R1.confg)

R1>

We will stop loading of saved configuration into RAM.

Password Implementation :

Router>

Router>enable

Router#conf t

#enable password 123

#enable secret 456

#line con 0

#password 789

#login

#exit

How to define local user at router?

R1(config)#username Shankar password xyz

#line con 0

#login local

#exit

Steps for router password recovery :

Power on the router

Press ctrl+pause break

Now router will enter into Rommon mode

Rommon1>confreg 0x2142 -> it will change NVRAM register value

Rommon2>reset

Now, router will prompt you to do initial configuration ?no

Router>enable

Router#copy startup-config running-config

R1#sh run

R1#conf t

R1(config)#line con 0

R1(config-line)#no password

R1(config-line)#no login

R1(config-line)#exit

R1(config)#no enable password

R1(config)#no enable secret

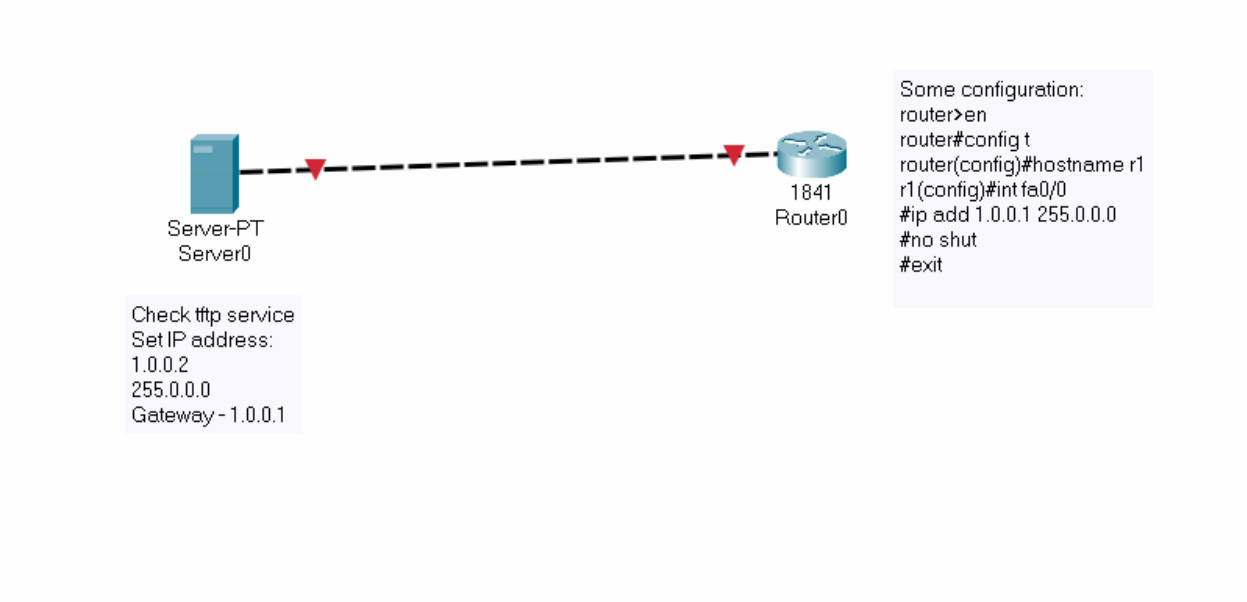
R1(config)#config-register ox2102

R1(config)#exit

R1#write memory

R1#reload

How to take back up of configuration file of a router?



Commands-

R1#copy startup-configtftp

Address of remote host?1.0.0.2

Destination file name[r1-confg]? --→ Press enter here

How to restore startup configuration file?

Router#copytftpstartup-config

Address of remote host?1.0.0.2

Destination file name[startup-config]? -→ Press enter here

How to copy IOS file of router?

Router#copy flash: tftp

Source file name? ----------→ Give name of IOS file

Address of remote host?1.0.0.2

Destination file name[same name as given above]? →Press enter here

How to transfer IOS file a router?

1. First keep IOS file at TFTP server
2. Set an IP address at server -→ 1.0.0.2
3. TFTP service must be on

Steps for router:-

Rommon1>tftpdnld

IP_ADDRESS=1.0.0.1

IP_SUBNET_MASK=255.0.0.0

IP_DEFAULT_GATEWAY=1.0.0.1

TFTP_SERVER=1.0.0.2

TFTP_FILE= →Give IOS file name which are available at TFTP server

Rommon>tftpdnld

→Press Y to upload IOS file

Switch Password Recovery :

Configuration is available in flash as config.text

We will rename this file to stop loading this file at the time of booting of switch.

1. Power off the switch.
2. Press Mode button and hold it.
3. Power on the switch.
4. It will bring the switch into rommon mode
5. Now, release the mode button
6. Rommon1>flash_init
   Rommon2>rename flash:config.text flash:config.patna
   Rommon3>dir flash:

..... config.patna
Rommon4>boot
Initial configuration? No
Switch>en
Switch#rename flash:config.patna flash:config.text
Switch#sh flash:
Config.text
Switch#copy startup-config system:running-config
S1#sh run
.....
.....
If required, change or remove password.
S1#write memory
S1#reload